Air Live®
Powered by OvisLink Corp.

SNMP-FSH2602MG v2

24 + 2-port Mixed Gigabit SNMP Managed Switch

User's Manual

Copyright & Disclaimer

No part of this publication may be reproduced in any form or by any means, whether electronic, mechanical, photocopying, or recording without the written consent of OvisLink Corp.

OvisLink Corp. has made the best effort to ensure the accuracy of the information in this user's guide. However, we are not liable for the inaccuracies or errors in this guide. Please use with caution. All information is subject to change without notice

All Trademarks are properties of their respective holders.

Table of Contents

1. Introduction 1

1.1 Overview 1

1.2 How to Use This Guide 1

1.3 Firmware Upgrade and Tech Support 2

1.4 Features 2

2. Installing the SNMP-FSH2602MG v2 4

2.1 Before You Start 4

2.2 Package Content 4

2.3 Optional Accessories 5

2.4 Knowing your SNMP-FSH2602MG v2 6

2.5 Hardware Installation 6

2.5.1 Attaching Rubber Feet 6
2.5.2 Rack-mounted Installation 7
2.5.3 Power On 8

2.6 LED Table 8

3. Configuring the SNMP-FSH2602MG v2 10

3.1 Important Information 10

3.2 Prepare your PC 10

3.3 Management Interface 11

3.4 Introduction to Web Management 14

3.4.1 Getting into Web Management 14

4. Web Management in SNMP-FSH2602MG v2 16

4.1 Menu Structure of SNMP-FSH2602MG v2 16

4.2 Port Status 17

4.3 Port Statistics 18

4.4 Administrator 19

4.4.1 IP Configuration 19
4.4.2 Switch Setting 20
4.4.3 Console Port Information 27
4.4.4 Port Controls 27
4.4.5 Trunking 28
4.4.6 Forwarding and Filtering 32

4.4.7 VLAN configuration....36
4.4.8 Spanning Tree....43
4.4.9 Port Mirroring....46
4.4.10 SNMP Management....48
4.4.11 Security Manager....49
4.4.12 802.1X....50
4.5 TFTP Update Firmware....53
4.6 Configuration Backup....54
4.7 Factory Default....55
4.8 System Reboot....56
4.9 Panel List....56
4.10 IP Stacking....56
5. Console Management in SNMP-FSH2602MG v2....58
5.1 Connecting to the Console Port....58
5.2 Login in the Console Interface....58
5.3 Main Menu....60
5.4 Function Description....61
5.4.1 Status and Counters....61
5.4.2 Switch Configuration....64
5.4.3 Protocol Related Configuration....85
5.4.4 System Reset Configuration....100
6. Application Example: VLAN Network....107
6.1 Application Environment....107
6.2 VLAN Configuration....108
6.2.1 Configuration of Port Based VLAN....108
6.2.2 Configuration of 802.1Q VLAN....110
7. Application Example: IGMP Snooping....114
7.1 Application Environment....114
7.2 Configuration of video server and client....115
7.2.1 Video Server....115
7.2.2 Video client....120
7.3 IGMP Snooping in SNMP-FSH2602MG v2....122
8. Troubleshooting....124
8.1 Incorrect connections....124
8.2 Diagnosing LED Indicators....125

8.3 Cabling.....125
9. Specifications.....126
10. Network Glossary 130

1 Introduction

1.1 Overview

The SNMP-FSH2602MG v2 is a multi-port Ethernet Switch that can be used to build high-performance switched workgroup networks. It is a store-and-forward device that offers low latency for high-speed networking. The SNMP-FSH2602MG v2 is targeted at workgroup, department or backbone computing environment.

1.2 How to Use This Guide

SNMP-FSH2602MG v2 is a SNMP managed Switch with many functions. It is recommended that you read through the entire user's guide whenever possible. The user guide is divided into different chapters. You should read at least go through the first 3 chapters before attempting to install the device.

Recommended Reading

Chapter 1: This chapter explains the basi information for SNMP-FSH2602MG v2. It is a must read.

Chapter 2: This chapter is about hardware installation. You should read through the entire chapter.

Chapter 3:

- **3.1 Important Information**: This section has information of default setting such as IP, Username, and Password.
- **3.3 Management Interface**: This section introduces Web management, and Console management.
- **3.4 Introduction to Web Management**: This section tells you how to get into the WebUI using HTTP.

Chapter 4: This chapter explains all of the management functions via Web management.

Chapter 5: This chapter explains all of the management functions via Console management.

Chapter 6: if any trouble in using SNMP-FSH2602MG v2, you can refer to this chapter

Chapter 7: This chapter show technical specification of SNMP-FSH2602MG v2.

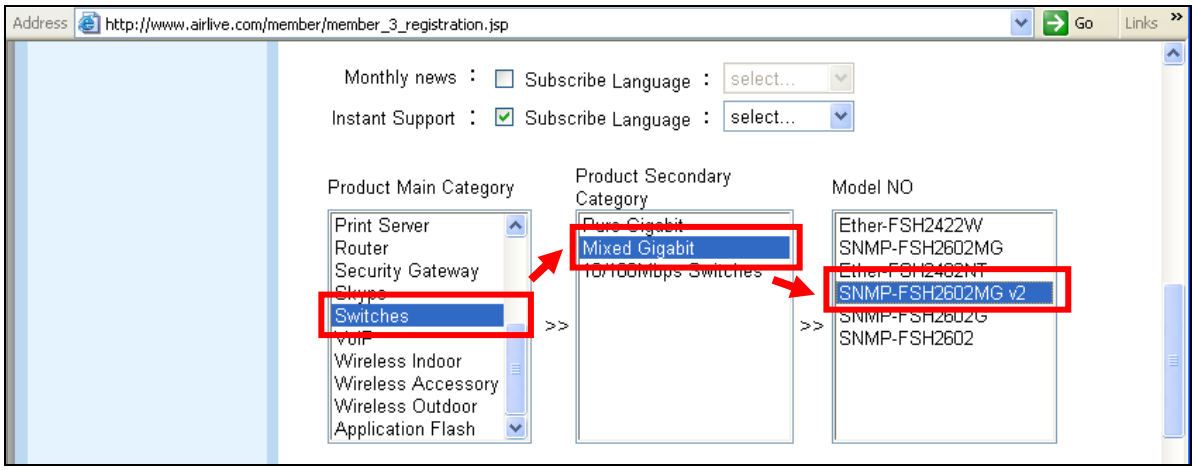
Chapter 8: Explanation on network technical terms from A to Z. Highly recommended for reference when you encounter an unfamiliar term.

1.3 Firmware Upgrade and Tech Support

If you encounter a technical issue that can not be resolved by information on this guide, we recommend that you visit our comprehensive website support at www.airlive.com. The tech support FAQ are frequently updated with latest information.

In addition, you might find new firmwares that either increase software functions or provide bug fixes for SNMP-FSH2602MG v2. You can reach our on-line support center at the following link:
http://www.airlive.com/support/support_2.jsp

Since 2009, AirLive has added the "Newsletter Instant Support System" on our website. AirLive Newsletter subscribers receives instant email notifications when there are new download or tech support FAQ updates for their subscribed airlive models. To become an AirLive newsletter member, please visit: http://www.airlive.com/member/member_3.jsp



1.4 Features

- Confirms to IEEE802.3 10BASE-T, 802.3u 100BASE-TX, 802.3ab 1000BASE-T, 802.3z Gigabit fiber
- 24 10/100 TX plus 2 Gigabit copper/Mini GBIC slot stackable intelligent switch
- High back-plane bandwidth 8.8Gbps

- 8K-entry MAC address table
- Management via single IP address
- IGMP support for Multi Media application
- Port mirror supported
- Support Port bandwidth control
- Supports GVRP function
- DHCP client supported
- Support Port Based VLAN /802 .1Q VLAN
- IEEE802.3x Flow control
  - Flow control for full duplex
  - Backpressure for half duplex
- Support IEEE802.3ad Port trunk with LACP
- Broadcast storm filter supported
- Support IEEE 802.1p class of service
- Support Port security
- IEEE 802.1d Spanning tree protocol supported
- Auto detect Gigabit copper and MINI GBIC
- Support IEEE 802.1x user authentication
- Support IP Stacking

2 Installing the SNMP-FSH2602MG v2

This chapter describes the hardware features and the hardware installation procedure for the SNMP-FSH2602MG v2. For software configuration, please go to chapter 3 for more details.

2.1 Before You Start

It is important to read through this section before you install the SNMP-FSH2602MG v2.

- The maximum cabling distance is 100 meters.
- Do not create a network loop.
- Always check the LED lights for troubleshooting

2.2 Package Content

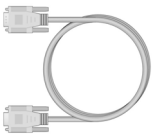
Unpack the contents of the SNMP-FSH2602MG v2 and verify them against the checklist below.

- One unit of SNMP-FSH2602MG v2
- Power Cord
- Four Rubber Feet
- RS-232 cable
- User Guide (CD-ROM)
- Quick Installation Guide
- Rack-mounted Kit

SNMP-FSH2602MG v2

Power Cord

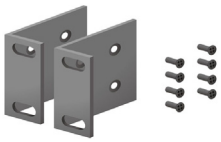
Four Rubber Feet



RS-232 cable

User Guide (CD-ROM)

Quick Installation Guide



Rack-mounted Kit

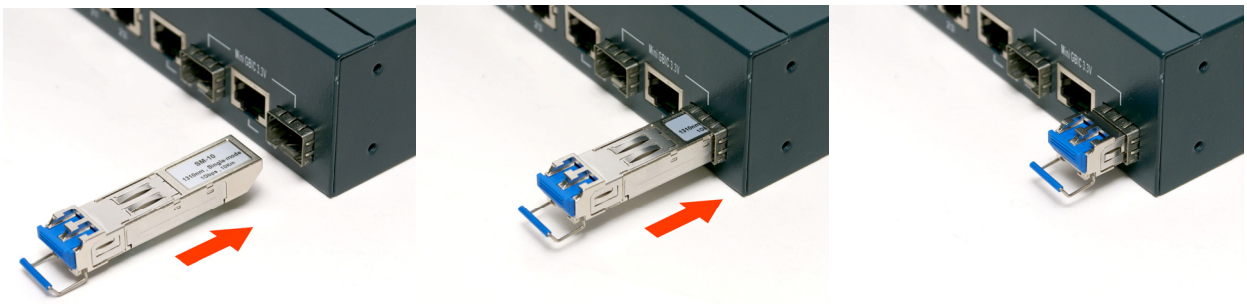
Compare the contents of your SNMP-FSH2602MG v2 package with the standard checklist above. If any item is missing or damaged, please contact your local dealer for service.

2.3 Optional Accessories

The SNMP-FSH2602MG v2 has the following optional accessories which you can purchase from AirLive

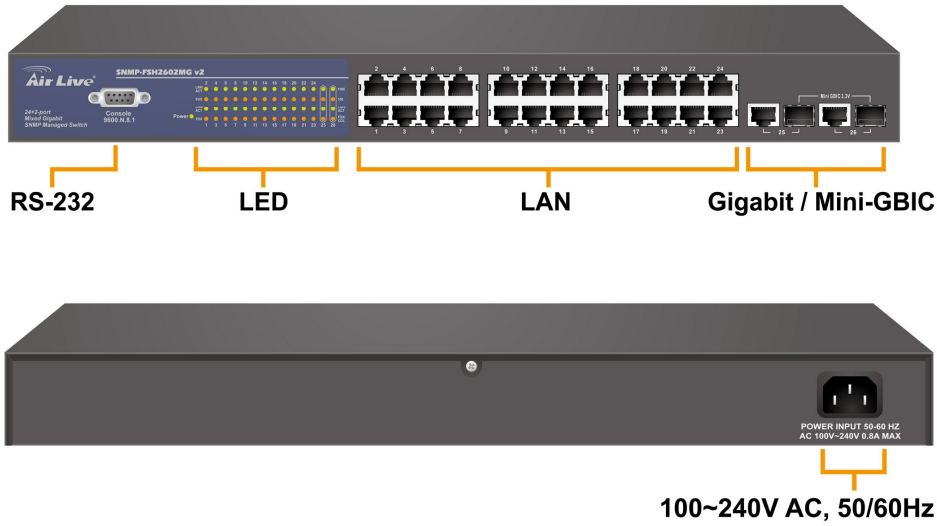
- 1000Base-SX MiniGBIC Transceiver (*Model: MGB-SX*) or 1000Base-LX MiniGBIC Transceiver (*Model: MGB-LX-10*) is for your SFP slots of SNMP-FSH2602MG v2, it allows you to use fiber cable for extending transmission distance.

Note: While installing MiniGBIC into SFP slot of SNMP-FSH2602MG v2, please notice the direction of MiniGBIC is correct, and make sure that MiniGBIC is indeed installed in the SNMP-FSH-2602MG v2.



2.4 Knowing your SNMP-FSH2602MG v2

Below are descriptions and diagrams of the product:



2.5 Hardware Installation

Set the SNMP-FSH2602MG v2 on a sufficiently large flat space with a power outlet nearby. The surface where you put your SNMP-FSH2602MG v2 should be clean, smooth, level and sturdy. Make sure there is enough clearance around the SNMP-FSH2602MG v2 to allow attachment of cables, power cord and allow air circulation.

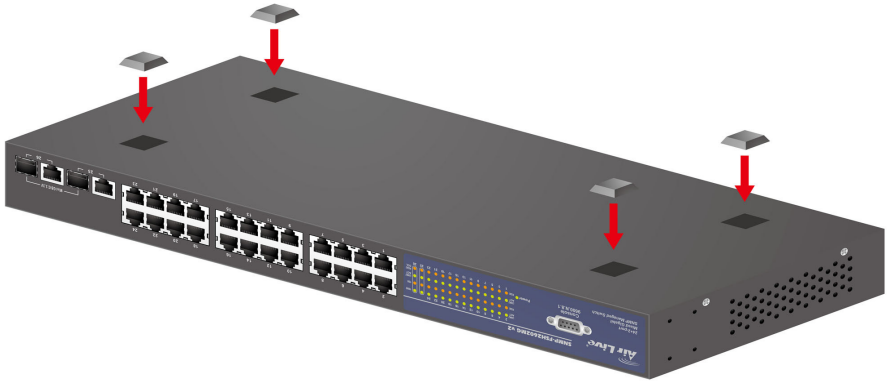
2.5.1 Attaching Rubber Feet

A. Make sure mounting surface on the bottom of the SNMP-FSH2602MG v2 is grease

and dust free.

B. Remove adhesive backing from your Rubber Feet.

C. Apply the Rubber Feet to each corner on the bottom of the SNMP-FSH2602MG v2. These footpads can prevent the Switch from shock/vibration.

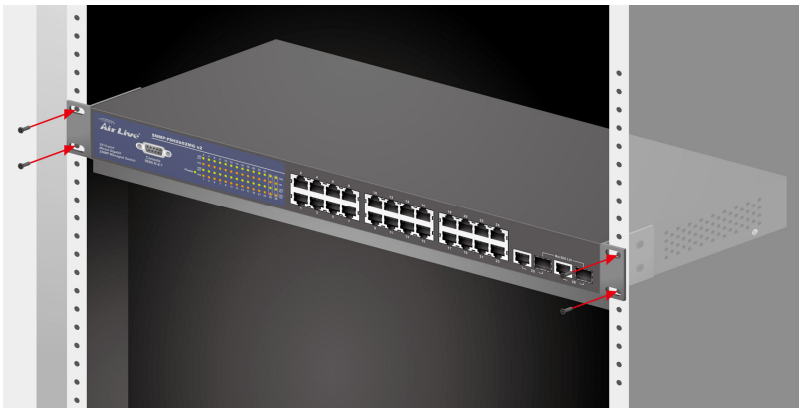


2.5.2 Rack-mounted Installation

The SNMP-FSH2602MG v2 comes with a rack-mounted kid and can be mounted in an EIA standard size, 19-inch Rack. The SNMP-FSH2602MG v2 can be placed in a wiring closet with other equipment. Perform the following steps to rack mount the SNMP-FSH2602MG v2:

A. Position one bracket to align with the holes on one side of the SNMP-FSH2602MG v2 and secure it with the smaller bracket screws. Then attach the remaining bracket to the other side of the SNMP-FSH2602MG v2.

B. After attached mounting brackets, position the SNMP-FSH2602MG v2 in the rack by lining up the holes in the brackets with the appropriate holes on the rack. Secure the SNMP-FSH2602MG v2 to the rack with a screwdriver and the rack-mounting screws.



Note: For proper ventilation, allow about at least 4 inches (10 cm) of clearance on the front and 3.4 inches (8 cm) on the back of the Switch. This is especially important for enclosed rack installation.

2.5.3 Power On

Connect the power cord to the power socket on the rear panel of the SNMP-FSH2602MG v2. The other side of power cord connects to the power outlet. The internal power supply of the SNMP-FSH2602MG v2 works with voltage range of AC in the 100-240VAC, frequency 50~60Hz. Check the power indicator on the front panel to see if power is properly supplied.

2.6 LED Table

The LED Indicators gives real-time information of systematic operation status. The following table provides descriptions of LED status and their meaning.

LED	Status	Description
Power	Green	Power On
	Off	Power is not connected

LNK/ACT	Green	The port is connecting with the device.
	Blink	The port is receiving or transmitting data.
	Off	No device attached.
FDX	Orange	The port is operating in Full-duplex mode.
	Off	In half-duplex mode
1000(Giga port) #25, #26 port	Green	In 1000Mbps connection speed
100(Giga port) #25, #26 port	Orange	In 100Mbps connection speed
LNK/ACT (Giga port) #25, #26 port	Green	The port is connecting with the device.
	Blink	The port is receiving or transmitting data.
	Off	No device attached
FDX/COL (Giga port) #25, #26 port	Orange	The port is operating in Full-duplex mode.
	Blink	Collision of Packets occurs in the port.
	Off	In half-duplex mode

3 Configuring the SNMP-FSH2602MG v2

The SNMP-FSH2602MG v2 offers many different types of management interface. You can configure through standard web browser (http), console (terminal), telnet, and SNMP management. In this chapter, we will explain SNMP-FSH2602MG v2's available management interfaces and how to get into them. Then, we will provide the introduction on Web Management and recommended initial settings. For detail explanations on Web Management functions, please go to Chapter 4. For Console interface, please go to Chapter 5.

3.1 Important Information

The following information will help you to get start quickly. However, we recommend you to read through the entire manual before you start. Please note the username and password are case sensitive.

- The default IP address is **192.168.10.1**
- The default Subnet Mask is **255.255.255.0**
- The default Gateway is **192.168.10.254**
- The default username is **airlive**
- The default password is **airlive**

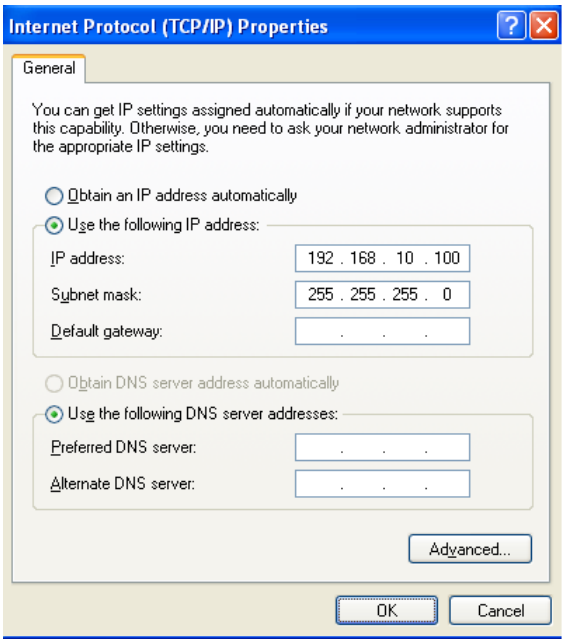
3.2 Prepare your PC

The SNMP-FSH2602MG v2 can be managed remotely by a PC through RJ-45 cable. The default IP address of the SNMP-FSH2602MG v2 is **192.168.10.1** with a *subnet mask* of 255.255.255.0. This means the IP address of the PC should be in the range of 192.168.10.2 to 192.168.10.254.

To prepare your PC for management with the SNMP-FSH2602MG v2, please do the following:

1. Connect your PC directly to the copper port of SNMP-FSH2602MG v2

2. Set your PC's IP address manually to 192.168.10.100 (or other address in the same subnet)


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
192 . 168 . 10 . 100
Subnet mask:
255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

You are ready now to configure the SNMP-FSH2602MG v2 by using your PC.

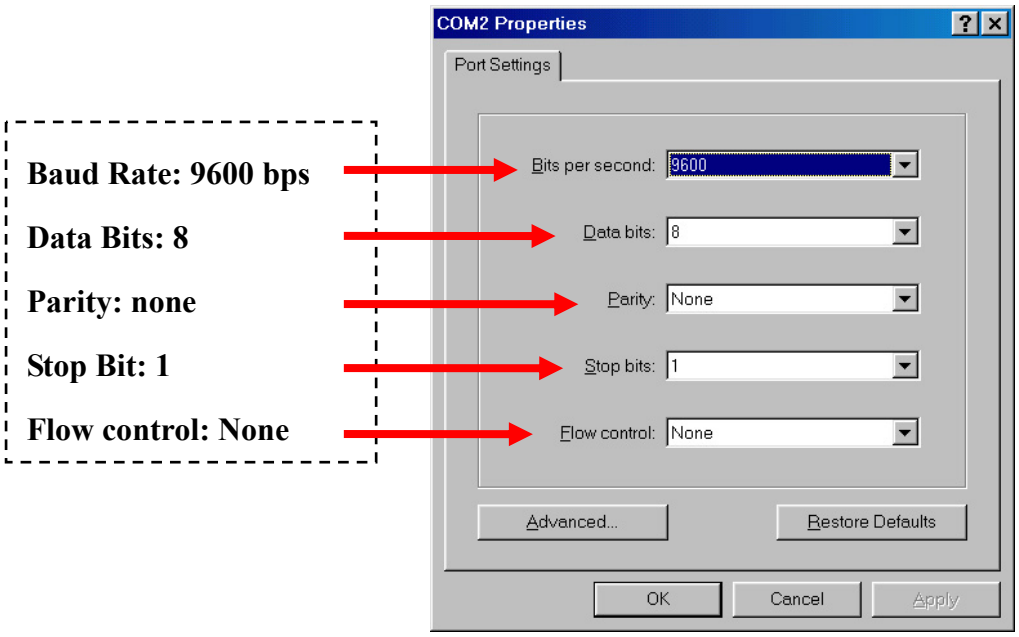
3.3 Management Interface

The SNMP-FSH2602MG v2 can be configured using on the management interfaces below:

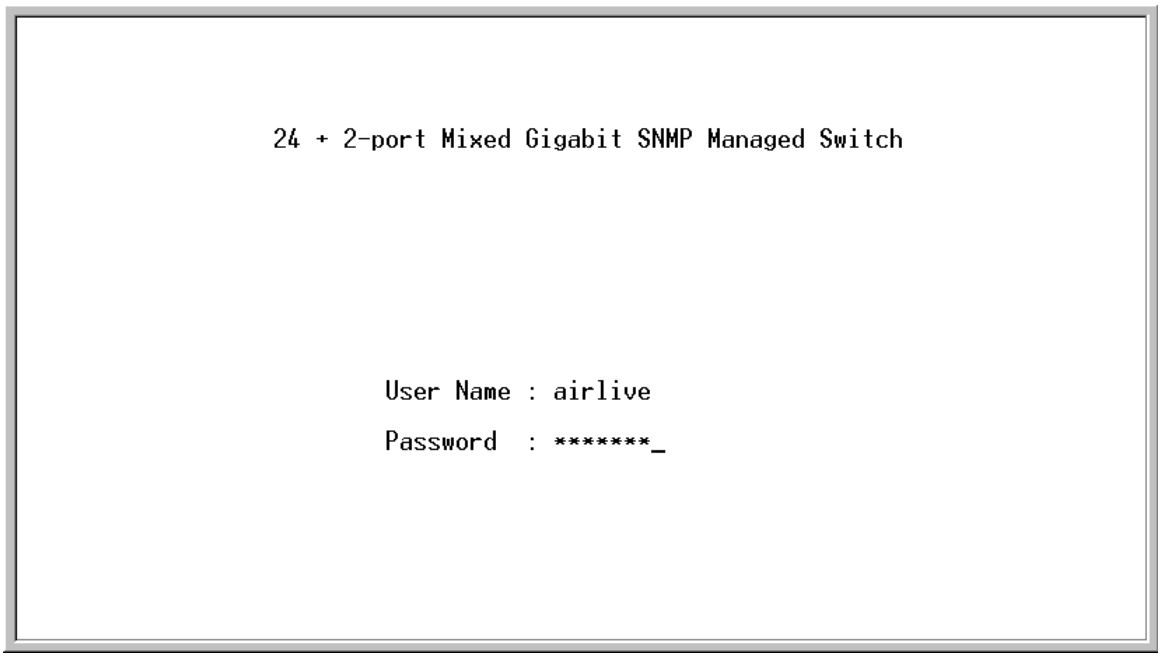
- **Web Management (HTTP)**: You can manage your SNMP-FSH2602MG v2 by simply typing its IP address in the web browser. Most functions of SNMP-FSH2602MG v2 can be accessed by web management inter face. We recommend using this interface for initial configurations. To begin, simply enter SNMP-FSH2602MG v2's IP address (default is 192.168.10.1) on the web browser. The default username and password are **airlive**.

- **Console Management (Terminal)**: SNMP-FSH2602MG v2 can be managed through terminal emulation program or **Hyper Terminal**.

  When the connection between SNMP-FSH2602MG v2 and PC is ready, turn on the PC and run a terminal emulation program or Hyper Terminal and configure its communication parameters to match the following default characteristics of the console port

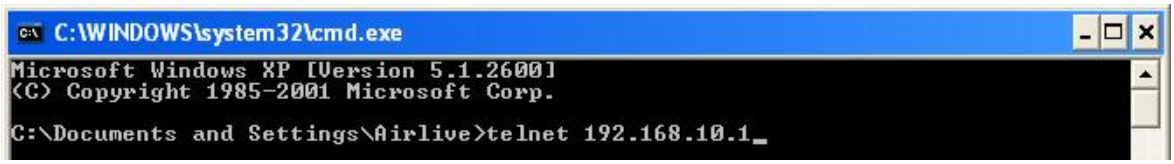


After finishing the parameter settings, click "**OK**". When the blank screen shows up, press Enter key to bring out the login prompt. Key in the "**airlive**"(default value) for the both User name and Password (use **Enter** key to switch), then press Enter key and the Main Menu of console management appears. Please see below figure for login screen.

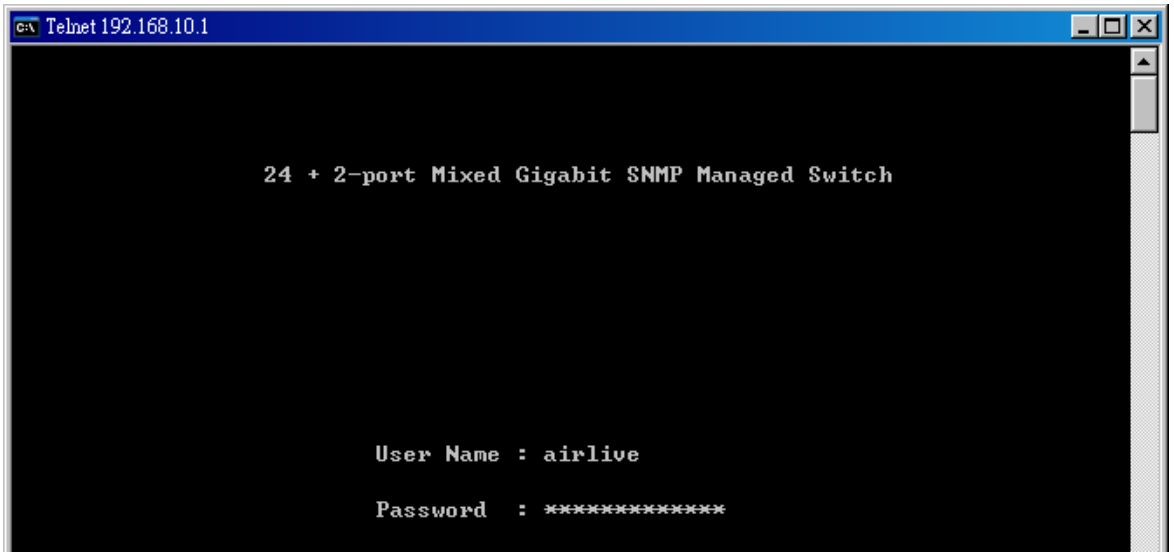


- **Telnet Management (Terminal)**: SNMP-FSH2602MG v2 can be managed through telnet. To use the telnet, please open the command line windows. Then type "telnet

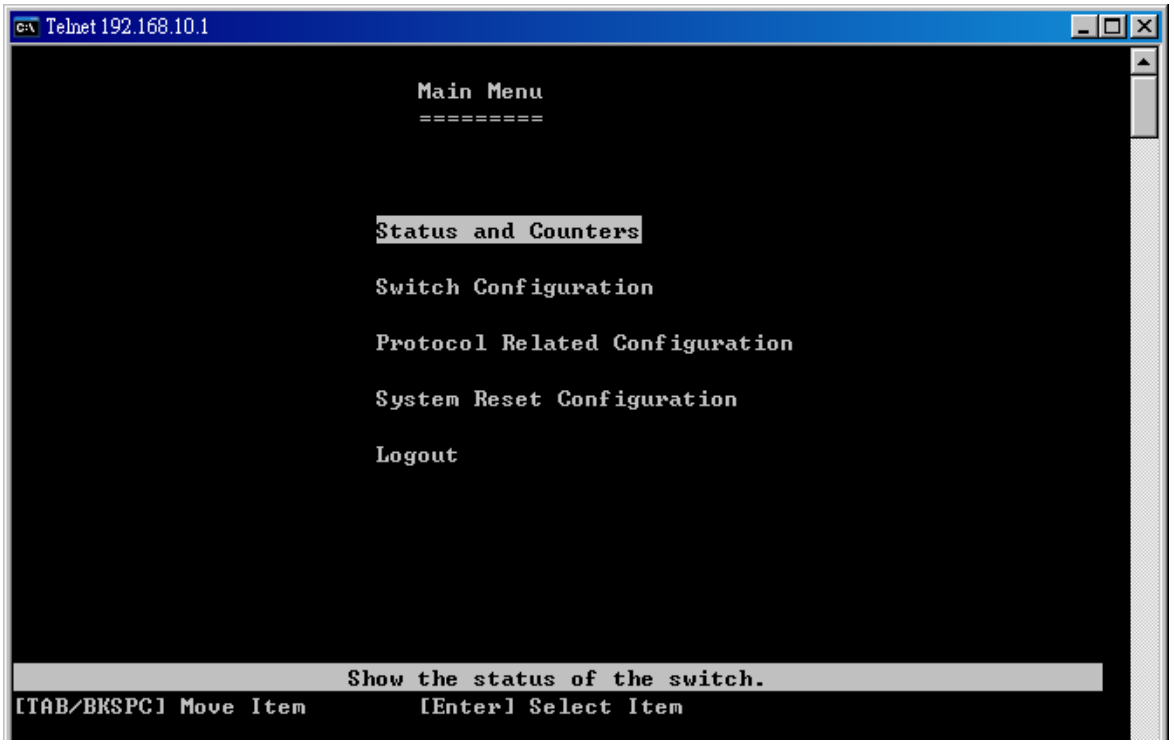
192.168.10.1" to start.



When asking for username and password, please enter "**airlive**".



Once entering username and password successfully, you will see main menu of configuration.



3.4 Introduction to Web Management

The SNMP-FSH2602MG v2 offers Web Management interfaces for users. Users can easily access and control SNMP-FSH2602MG v2 via web browsers. The only difference is HTTPS are encrypted for extra security. Therefore, we will discuss them together as "Web Management" on this guide.

The Web-Based Management supports Internet Explorer 5.0. It is based on Java Applets with an aim to reduce network bandwidth consumption, enhance access speed and present an easy viewing screen.

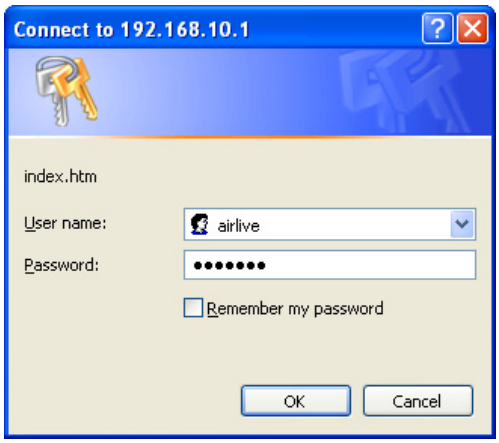
Note: By default, IE5.0 or later version does not allow Java Applets to open sockets. The user has to explicitly modify the browser setting to enable Java Applets to use network ports.

3.4.1 Getting into Web Management

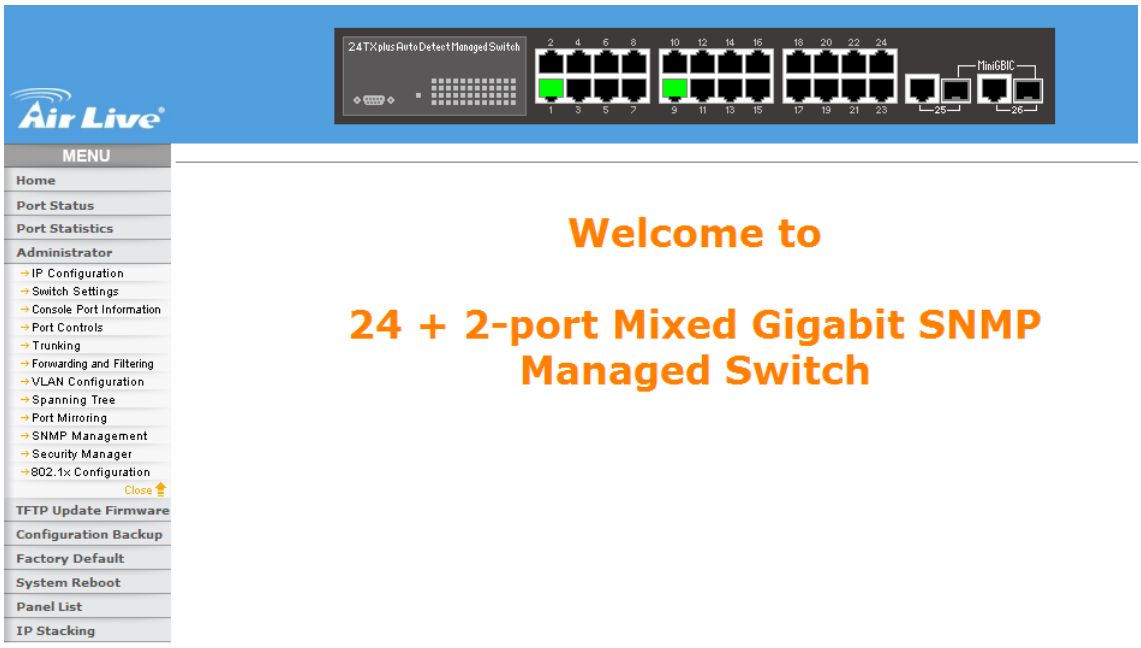
Web Management (HTTP)

1. Launch the Internet Explorer.
2. Type http://192.168.10.1. Press "**Enter**".

3. The login screen appears.
4. Key in the user name and password. The default user name and password is "**airlive**".



5. Click “**Enter**” or ”**OK**”, then the home screen of the Web-based management appears.

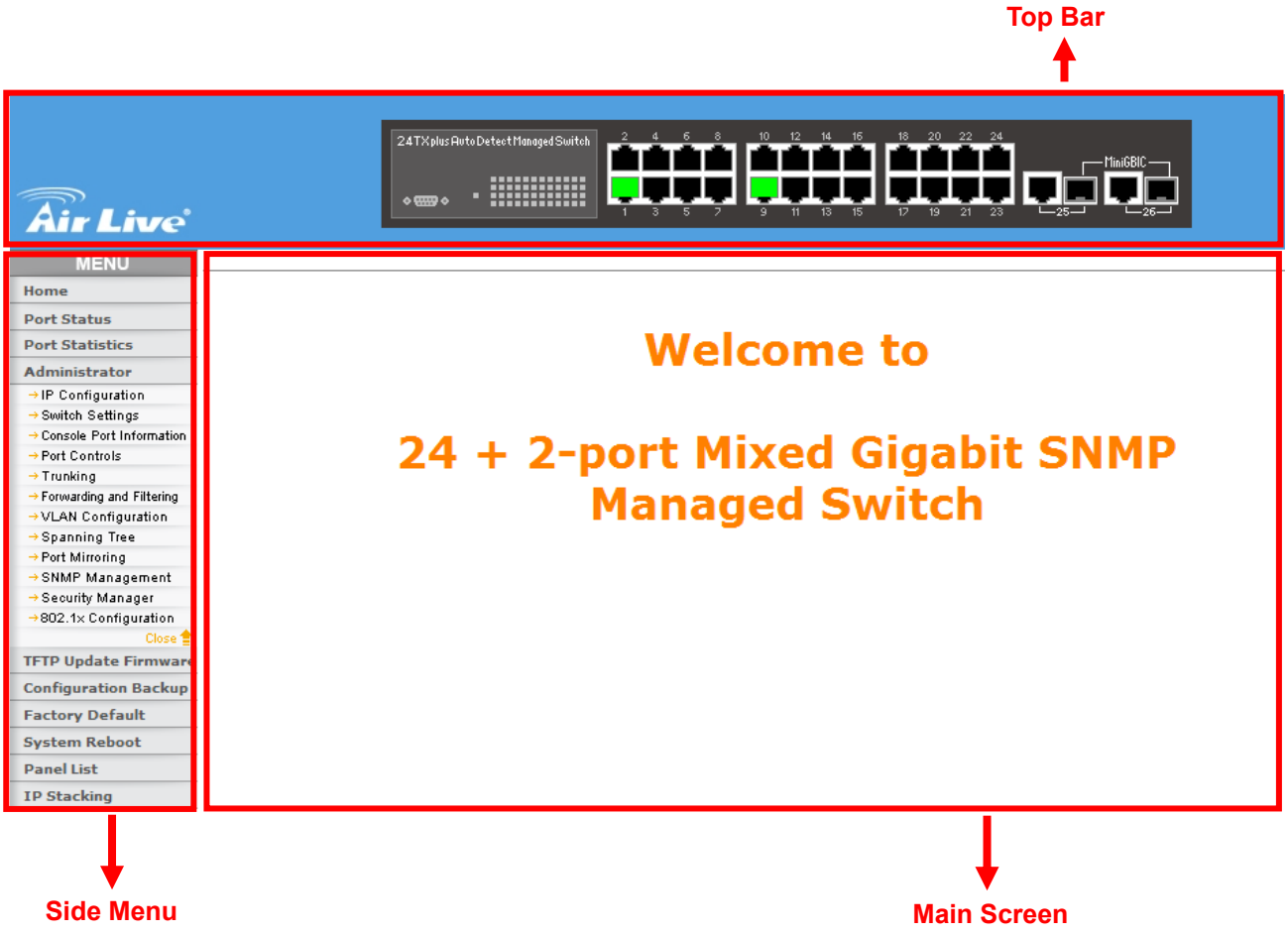


4 Web Management in SNMP-FSH2602MG v2

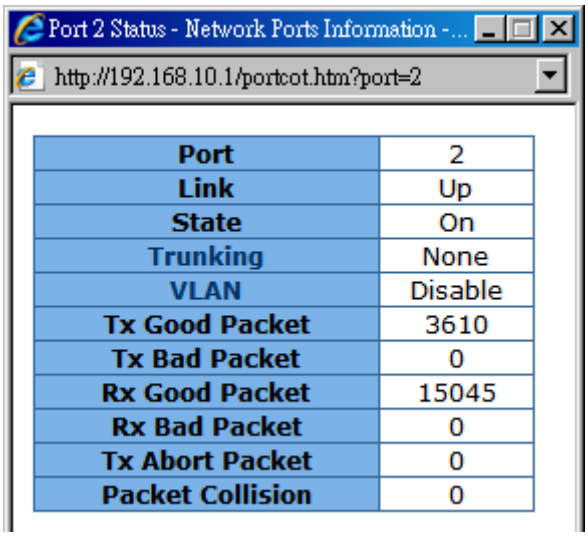
In this chapter, we will explain all settings in web management interface. Please be sure to read through Chapter 3's "*Introduction to Web Management*" first.

4.1 Menu Structure of SNMP-FSH2602MG v2

The web management menu of SNMP-FSH2602MG v2 is divided into 3 parts: *Top Bar, Side Menu Bar*, and *Main Screen*.



- **Top Bar**: It display panel GUI. You can direct click the port on the Switch figure on the top of web page. Then, you will see the port information.



Port	2
Link	Up
State	On
Trunking	None
VLAN	Disable
Tx Good Packet	3610
Tx Bad Packet	0
Rx Good Packet	15045
Rx Bad Packet	0
Tx Abort Packet	0
Packet Collision	0

- **Side Menu:** All management functions will show in Side Menu, you can choose any one of them to configure its setting. The detailed introduction for all management function will explain in below chapters.
- **Main Screen**: Once choosing any function of Side Menu, the configuration page of the function will show in Main Screen. You can configure the function by instruction of manual.

Note:

You can click "**Help**" button when you have any configuration question during configuring.

4.2 Port Status

In Port status, you can view every port status that depended on user setting and the negotiation result.

1. **Link:** "Down" is "No Link". "UP" is "Link".
2. **State:** Display port statuses "disable" or "enable". "Unlink" will be treated as "off".
3. **Auto Negotiation:** Display the auto negotiation mode: auto/force/Nway-force. "Config" means the value that user configured. "Actual" means the current value of the port.
4. **Speed Duplex:** Display port connection speed. "Config" means the value that user configured. "Actual" means the current value of the port.
5. **Flow Control:** Display the flow control status is "enable" or "disable" in full duplex mode. "Config" means the value that user configured. "Actual" means the current value

of the port.

6. **Back Pressure:** Display the Back Pressure status setting. “Config” means the value that user configured. “Actual” means the current value of the port.
7. **Bandwidth:** Display the port incoming and outgoing bandwidth.
8. **Priority:** Display the port static priority status is “High” or “Low” or “Disable”.
9. **Port Security:** Display the port security is “enable” or “disable”.

4.3 Port Statistics

The following information provides a view of the current port statistic information.

Click “Clear” button to clean all counts.

Port Statistics

Port	Type	Link	State	Tx Good Packet	Tx Bad Packet	Rx Good Packet	Rx Bad Packet	Tx Abort Packet	Packet Collision
Port.01	100TX	Down	Enable	0	0	0	0	0	0
Port.02	100TX	Up	Enable	3990	0	16068	0	0	0
Port.03	100TX	Down	Enable	0	0	0	0	0	0
Port.04	100TX	Down	Enable	0	0	0	0	0	0
Port.05	100TX	Down	Enable	0	0	0	0	0	0
Port.06	100TX	Down	Enable	0	0	0	0	0	0
Port.07	100TX	Down	Enable	0	0	0	0	0	0
Port.08	100TX	Down	Enable	0	0	0	0	0	0
Port.09	100TX	Down	Enable	0	0	0	0	0	0
Port.10	100TX	Down	Enable	0	0	0	0	0	0
Port.11	100TX	Down	Enable	0	0	0	0	0	0
Port.12	100TX	Down	Enable	0	0	0	0	0	0
Port.13	100TX	Down	Enable	0	0	0	0	0	0
Port.14	100TX	Down	Enable	0	0	0	0	0	0
Port.15	100TX	Down	Enable	0	0	0	0	0	0
Port.16	100TX	Down	Enable	0	0	0	0	0	0
Port.17	100TX	Down	Enable	0	0	0	0	0	0
Port.18	100TX	Down	Enable	0	0	0	0	0	0
Port.19	100TX	Down	Enable	0	0	0	0	0	0
Port.20	100TX	Down	Enable	0	0	0	0	0	0
Port.21	100TX	Down	Enable	0	0	0	0	0	0
Port.22	100TX	Down	Enable	0	0	0	0	0	0
Port.23	100TX	Down	Enable	0	0	0	0	0	0
Port.24	100TX	Down	Enable	0	0	0	0	0	0
Port.25	Auto	Down	Enable	0	0	0	0	0	0
Port.26	Auto	Down	Enable	0	0	0	0	0	0

Clear

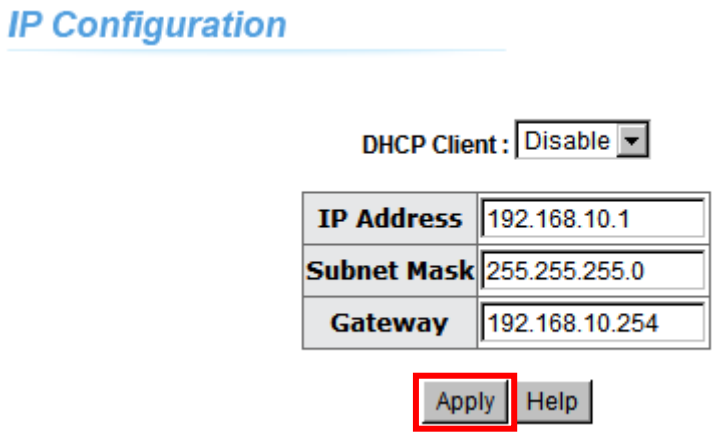
4.4 Administrator

In Administrator function, it provides the following functions:

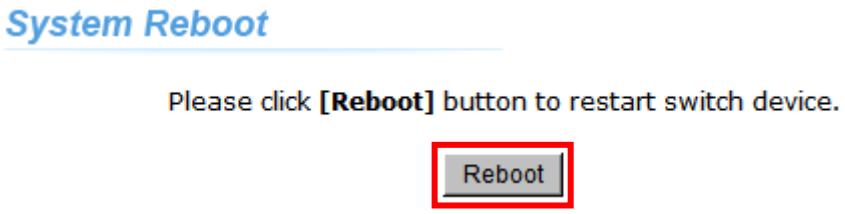
IP Configuration, Switch Settings, Console Port Information, Port Controls, Trunking, Forwarding and Filtering, VLAN Configuration, Spanning Tree, Port Mirroring, SNMP Management, Security Manager, and 802.1x Configuration.

4.4.1 IP Configuration

User can configure the IP Settings and DHCP client function, then clicks "**Apply**" button to apply your setting.



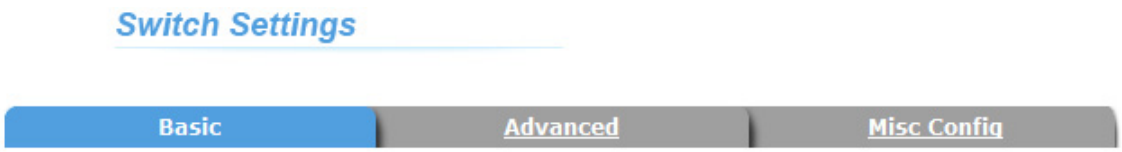
After changing the IP address, you must reboot SNMP-FSH2602MG v2.



- **DHCP Client:** Disable or enable the DHCP client function. Once enabling "**DHCP Client**" function, SNMP-FSH2602MG v2 will get IP address by DHCP server.
- **IP Address:** Assign the switch IP address. The default IP is 192.168.10.1.
- **Subnet Mask:** Assign the switch IP subnet mask. The default IP is 255.255.255.0
- **Gateway:** Assign the switch gateway. The default Gateway IP is 192.168.10.254.

4.4.2 Switch Setting

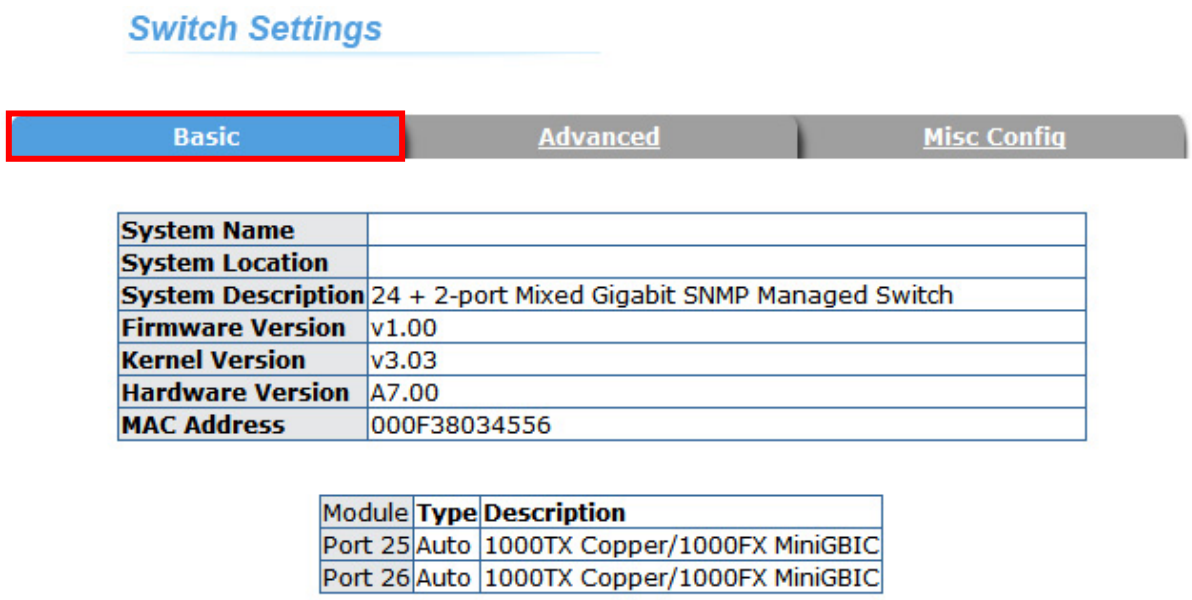
In this page, it has three parts of setting: **Basic**, **Advance**, and **Misc Config**. We will describe the configure detail in following.



4.4.2.1 Basic

In **Basic** setting, it displays the switch basic information.

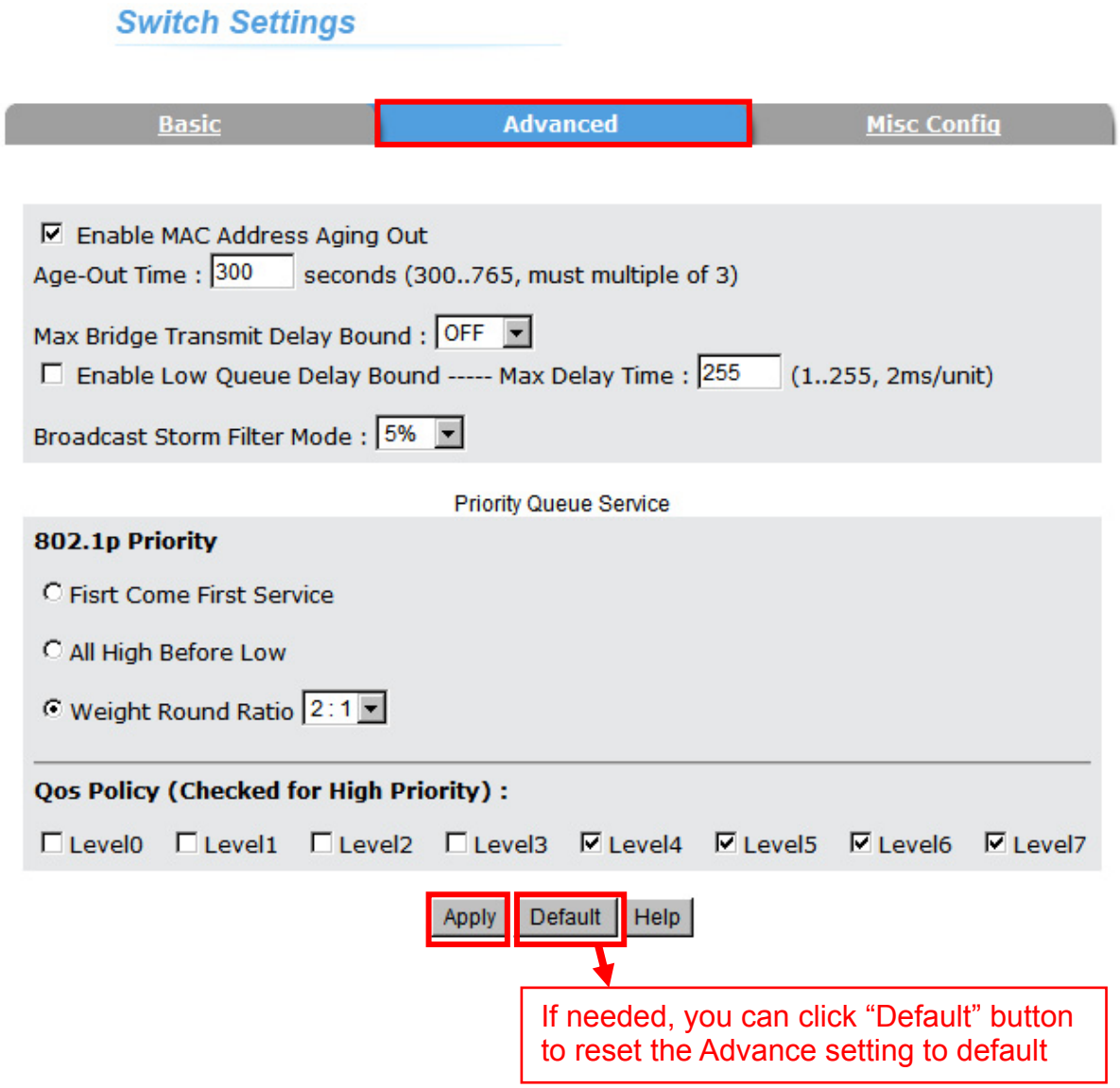
- **System Name:** Display the name of switch.
- **System Location:** Display the switch physical location.
- **System Description:** Display the description of switch.
- **Firmware Version:** Display the switch's firmware version.
- **Kernel Version:** Display the kernel software version.
- **Hardware version:** Display the switch hardware version.
- **MAC Address:** Display the unique hardware address assigned by AirLive
- **Module:** Display the MiniGBIC information.



4.4.2.2 Advanced

In **Advanced** setting, it has two sections: **MAC Table Address Entry** and **Priority Queue Service.** After configuring, click "**Apply**" button to complete the configuration.

Note: If you want to reset the **Advanced** setting to default, please click "Default" button in the bottom of the page.

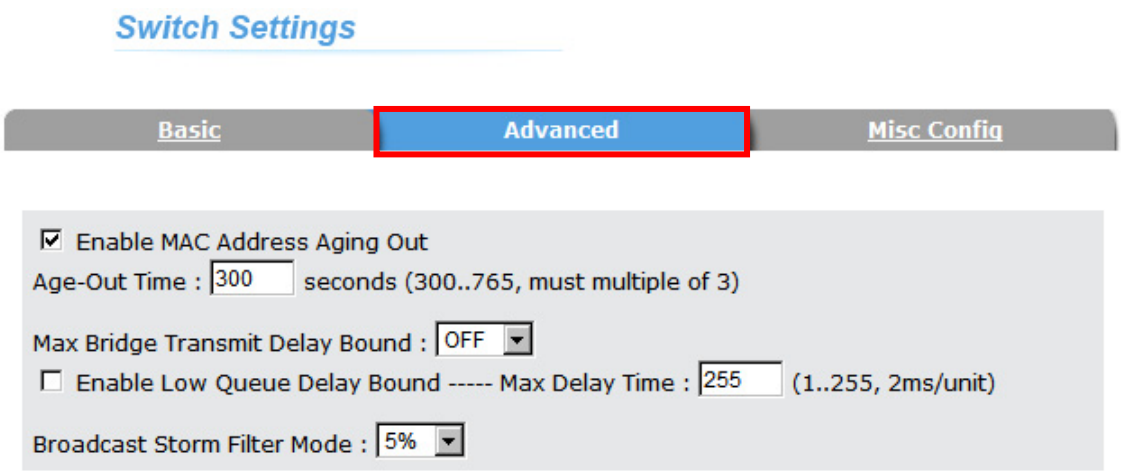

Switch Settings
Basic
Advanced
Misc Config
Enable MAC Address Aging Out
Age-Out Time : 300 seconds (300..765, must multiple of 3)
Max Bridge Transmit Delay Bound : OFF
Enable Low Queue Delay Bound ----- Max Delay Time : 255 (1..255, 2ms/unit)
Broadcast Storm Filter Mode : 5%
Priority Queue Service
802.1p Priority
Fisrt Come First Service
All High Before Low
Weight Round Ratio 2 : 1
Qos Policy (Checked for High Priority) :
Level0 Level1 Level2 Level3 Level4 Level5 Level6 Level7
Apply
Default
Help
If needed, you can click “Default” button to reset the Advance setting to default

- **Enable MAC address Aging Out:** Switch has one MAC table which can record or update relation of MAC and port. Once other packets having the same destination are transmitted, Switch can easily know which path is right. It can save system resource of the Switch and decrease times of packet collision. However, the memory of the Switch is limited, MAC table needs to drop some inactive MAC to learn active MAC address continuously, so it is necessary to configure MAC table aging time.
  - **Age-out Time:** Fill in the number of seconds that an inactive MAC address remains in the Switch's address table. The valid range is 300~765 seconds (must be multiple of 3). The default is 300 seconds.
- **Max Bridge Transmit Delay Bound:** Limit the packets queuing time in Switch. If enabled, the packets whose queuing time exceed your setting will be dropped. The valid value is 1sec, 2 sec, 4 sec and off. The default is OFF
  - **Enable Low Queue Delay Bound:** Limit queuing time of low priority packets in Switch. If the low priority packets which time of staying in Switch exceed Max Delay Time, it will be sent. The valid range is 1~255 ms.

NOTE: Please make sure that “Max bridge transit delay bound” is enabled before enabling Delay Bound, because “Enable Low Queue Delay Bound” must be worked under situation of “Max bridge transit delay bound control is enabled”.

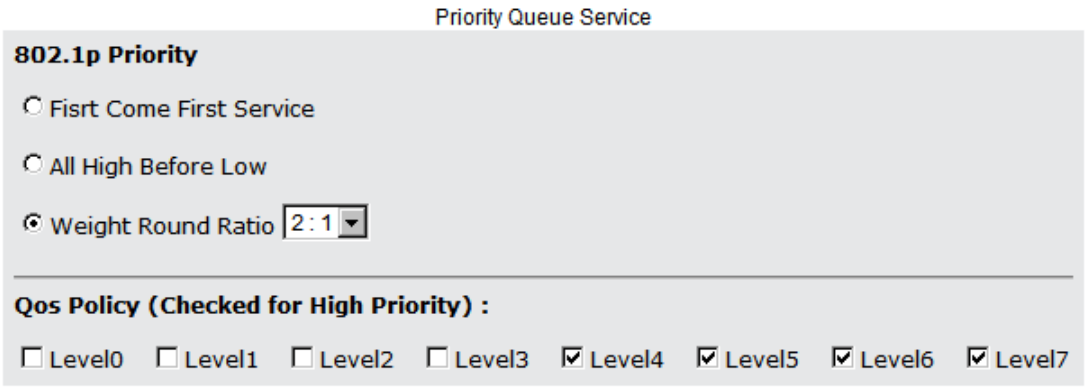
- **Broadcast Storm Filter:** A broadcast storm means that your network is overwhelmed with constant broadcast or multicast traffic. It will lead to a complete loss of network connectivity eventually. Therefore, filter function can protect your network against broadcast storms.

  Enable it and set the upper threshold for individual ports. The threshold is the percentage of the port's total bandwidth used by broadcast traffic. When broadcast transmit threshold for a port is reached to your threshold value, broadcast storm filter becomes active and drops all broadcast traffic. The valid threshold value is 5%, 10%, 15%, 20%, 25% and off.


Switch Settings
Basic
Advanced
Misc Config
Enable MAC Address Aging Out
Age-Out Time : 300 seconds (300..765, must multiple of 3)
Max Bridge Transmit Delay Bound : OFF
Enable Low Queue Delay Bound ----- Max Delay Time : 255 (1..255, 2ms/unit)
Broadcast Storm Filter Mode : 5%

- **Priority Queue Service settings:** There are many different applications, users, or data flows in a real network environment. However, the network capacity is limited, you have to keep some network services in good performance such as real-time streaming multimedia over IP or on-line games. Therefore, you can use priority mechanism to prioritize your network services. You have three kinds of priority queue service type to select.
  - **First Come First Service:** The sequence of packets sent is depended on arrive order.
  - **All High before Low:** The high priority packets are sent before low priority packets.
  - **Weighted Round Ratio:** Select the preference given to packets in the switch's high-priority queue. These options represent the number of high priority packets sent before one low priority packet is sent. For example, “5 High: 1 Low” means that the switch sends 5 high priority packets before sending 1 low priority packet. The valid ratio is 2:1, 3:1, 4:1, 5:1, 6:1 and 7:1.

- **Qos Policy: High Priority Levels:** 0~7 priority level can map to high or low queue. Once some levels are checked, it means that they have high priorities.



4.4.2.3 Misc Config

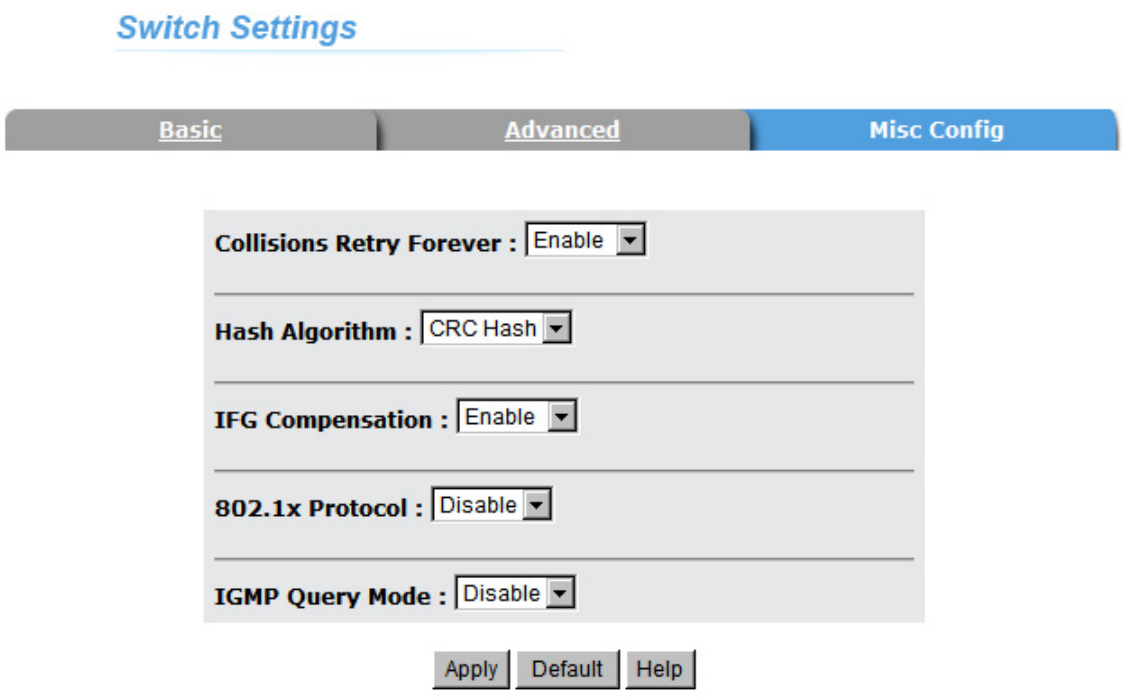
- **Collisions Retry Forever: "Disable"** – In half duplex, if collision happens, Switch will retry 48 times and then drop frame. Otherwise, if collision happens, the Switch will retry forever when "**Enable**".
- **Hash Algorithm:** CRC Hash or Direct Map for MAC address learning algorithm. After selecting one of both, chipset will learn MAC address according to your selected algorithm.
- **IFG Compensation:**

  Ethernet devices must allow a minimum idle time between transmission of Ethernet frames known as the **interframe gap** (IFG). This idle time gives the network media a chance to stabilize, and other network components to process the frame. The minimum interframe gap is 96 bit times (the time it takes to transmit 96 bits of raw data on the medium), which is 9.6 µs for 10 Mbit/s Ethernet, 960 ns for 100 Mbit/s Fast Ethernet, 96 ns for 1 Gbit/s (gigabit) Ethernet.

  Generally, the interframe gap is not always 96 bit frames, if it is less than 96 bit times, it will occur that transmission speed of SNMP-FSH2602MG v2 would be over 100/1000Mbps. If SNMP-FSH2602MG v2 transmit frames at a more than 100Mbps rate that causes some 10/100Mbps device to enter into a state of congestion (i.e. no buffer space remaining to receive additional frames), 10/100Mbps device may transmit a Pause frame which halt the transmission of the sender for a specified period of time. The flow control mechanism would begin to prevent from packet loss. User can select "Enable" or "Disable" to IFG Compensation.
- **802.1x Protocol:** It provides an authentication mechanism to devices wishing to attach to a LAN, either establishing a point-to-point connection or preventing it if authentication fails. Use can enable or disable 802.1x protocol. Once enabled, you can configure 802.1x setting in another web.
- **IGMP Query Mode:** Recognizes different queries from clients or servers to decide

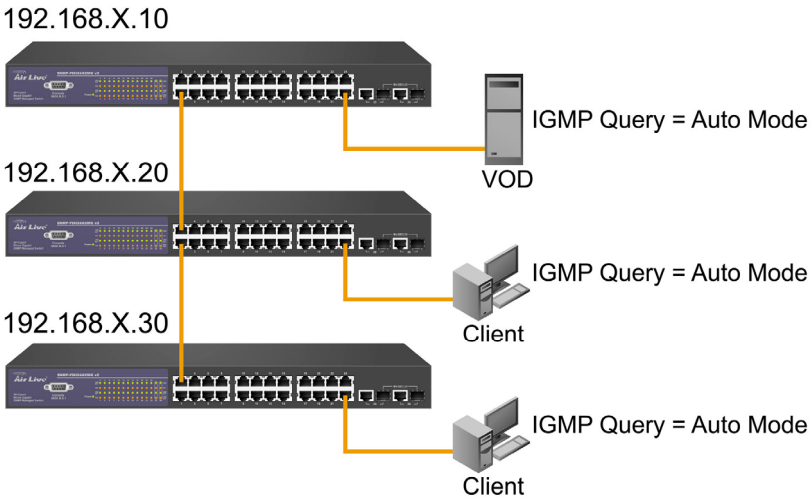
which Query will be the first priority. The modes are:

a. **Auto Mode:** Chooses the switch that has the smallest IP address to be set for the IGMP Query mode.
b. **Enable Mode:** Enables the switch to be the IGMP Querier.
c. **Disable Mode:** Disables all other switches from being the IGMP Querier.

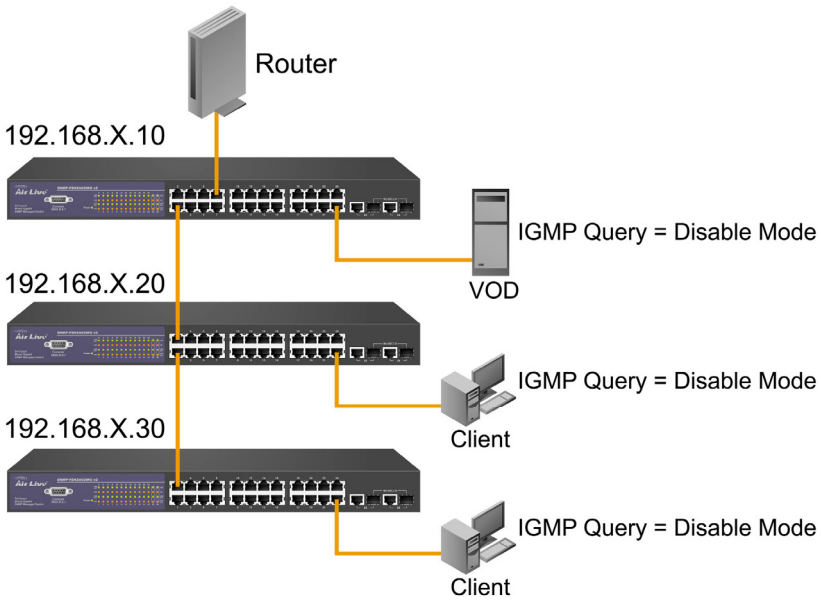


The following three topologies explain how IGMP Query works and to be configured within a network:

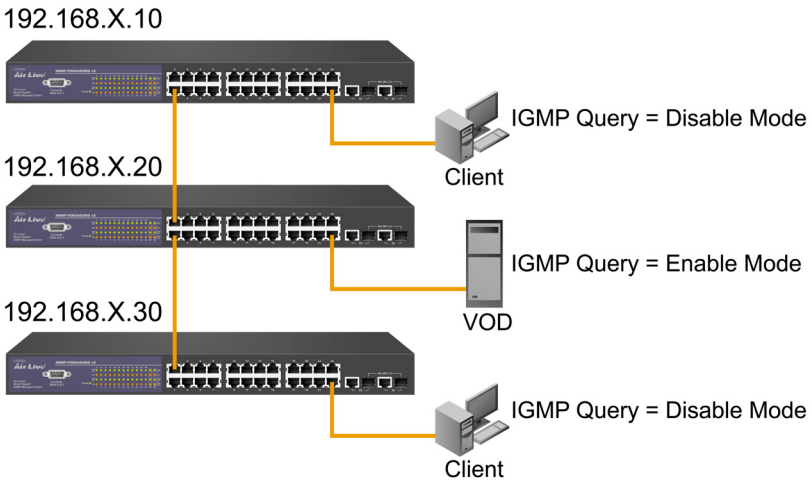
1. Auto mode needs to be enabled when the router's IP address is smaller than other switches in the subnet.



2. IGMP needs to be enabled when the router's IP address is not smaller than other switches in the subnet. This Router supports IGMP protocol, but IGMP has to be enabled, and the Router has to be the Querier.



3. The following topology must be set when the IP address of the switch is not the smallest in the subnet. The network will cause a multi-cast storm from the IGMP client report if it is in Auto mode. All switches must be in disable mode when the VOD server is configured for IGMP Querier.



Note: It is suggested that the VOD server switch have the smallest IP address.

4.4.3 Console Port Information

Console is a standard UART interface to communicate with Serial Port. User can use windows HyperTerminal program to link the switch. Please refer to **Chapter 5 Console Management** for detail steps.

Console port information shows as follow:

Bits per seconds: 9600

Data bits: 8
Parity: none
Stop Bits: 1
Flow control: none

Console Port Information

Baud Rate (bps)	9600
Parity Check	none
Data Bits (bit)	8
Stop Bits (bit)	1
Flow Control	none

4.4.4 Port Controls

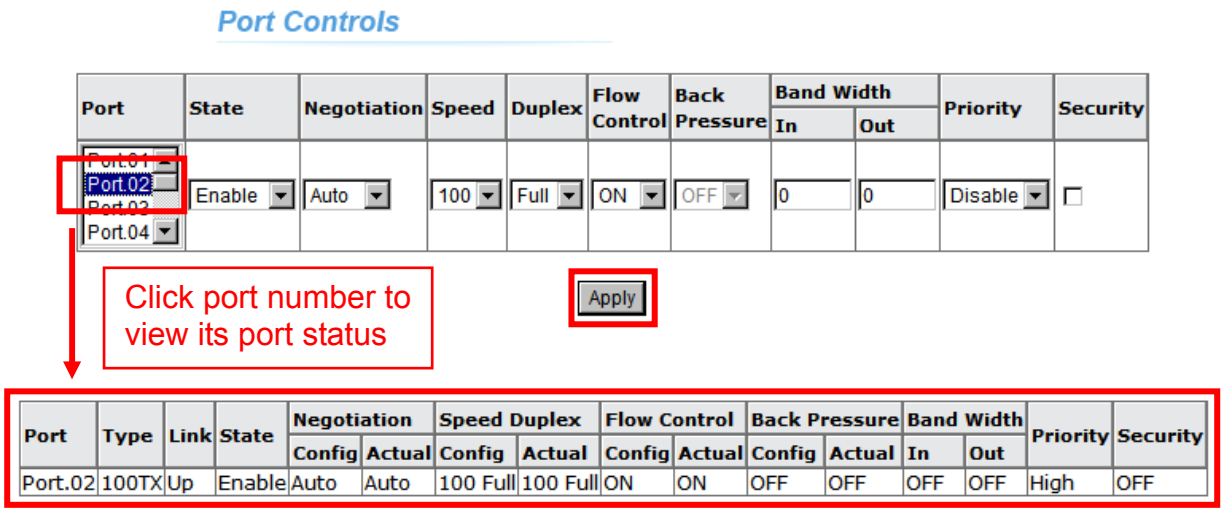
In the page, you can change the port status port by port as your needs.

1. Select the port by scrolling the list in **Port** column.
2. **State:** User can disable or enable this port control.
3. **Negotiation:** User can set negotiation mode as Auto or Force on port 1 to port 24, and only Auto on port 25 and port 26.
4. **Speed:** User can set speed as 10Mbps or 100Mbps on port 1 to port 24, and only 1000Mbps on port 25 and port 26.
5. **Duplex:** Set Full-Duplex or Half-Duplex mode of the port. When in Full-Duplex mode, user can configure **Flow control**; When in Half-Duplex mode, user can configure **Back Pressure**.
6. **Flow control:** Set flow control function as **ON** or **OFF** in Full Duplex mode.
7. **Back Pressure:** Set Back Pressure as **ON** or **OFF** in Half Duplex mode.
8. **Band Width:** The port1 to port 24 supports port ingress and egress rate control. For example, assume port 1 speed is 10Mbps, users can set it's effective egress rate is

1Mbps, ingress rate is 500Kbps. The switch will perform flow control or Back Pressure to confine the ingress rate to meet the specified rate.

- **In:** fill in the port effective ingress rate. The valid range is 0 ~ 999. The unit is 100K. "0" means disable rate control. "1 ~ 999" means valid rate value.
- **Out:** fill in the port effective egress rate. The valid range is 0~999. The unit is 100K. "0" means disable rate control. "1 ~ 999" means valid rate value.

9. **Priority:** This static priority is based on port, if you set the port as high priority, incoming frames from this port always are high priority frame.
10. **Security:** When the port is in security mode, the port will be "locked" without permission of address learning. Only the incoming packets with static MAC addresses already existing in the address table can be forwarded normally. User can disable the port from learning any new MAC addresses, and then use the Static MAC addresses (introduce in below pages) function to define a list of MAC addresses that can use the secure port.
11. Click "**Apply**" button to apply all configuration.
12. When you select the port, you can see port's current configuration value which shows in below column.



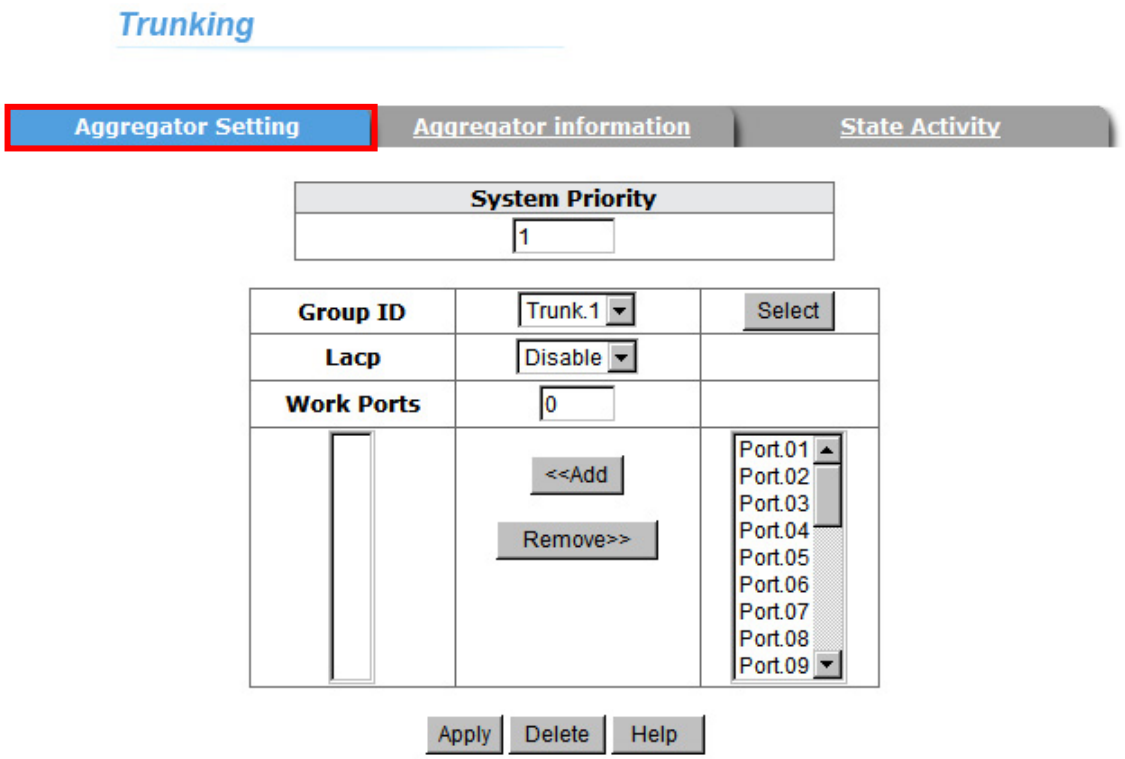
4.4.5 Trunking

Link Aggregation Control Protocol (LACP) provides a standardized means for exchanging information between Partner Systems on a link to allow their Link Aggregation Control instances to reach agreement on the identity of the Link Aggregation Group to which the link belongs, move the link to that Link Aggregation Group, and enable its transmission and reception functions in an orderly manner. Link aggregation lets you group up to eight consecutive ports into a single dedicated connection. This feature can expand bandwidth to

a device on the network. **LACP operation requires full-duplex mode,** please refers to IEEE 802.3ad for more detail information.

4.4.5.1 Aggregator setting

1. **System Priority:** A value used to identify the active LACP. The switch with the lowest value has the highest priority and is selected as the active LACP.
2. **Group ID:** There are seven trunk groups for users to configure. Choose the "**Group ID**" and click "**Select**" button.
3. **LACP:** If enabled, the group is LACP static trunk group. If disabled, the group is local static trunk group. All ports support LACP dynamic trunking group. If connecting to the device that also supports LACP, the LACP dynamic trunking group will be created automatically.
4. **Work ports:** Max four ports can be aggregated at the same time. If it is LACP static trunk group, the exceed ports are standby and able to aggregate if work ports fail. If it is local static trunk group, the number must be as same as the group member ports.
5. Select the ports to join the trunk group. Max four ports can be aggregated at the same time. Select the port and click "**Add**" button to add the port. To remove ports, just select the port and click "**Remove**" button.
6. If LACP is enabled, you can configure LACP Active/Passive status in each port on **State Activity** page.
7. Click "**Apply**" button to apply your Trunking configuration.
8. You also can use "**Delete**" button to delete Trunk group. Just select the Group ID and click "**Delete**" button to apply your delete action.



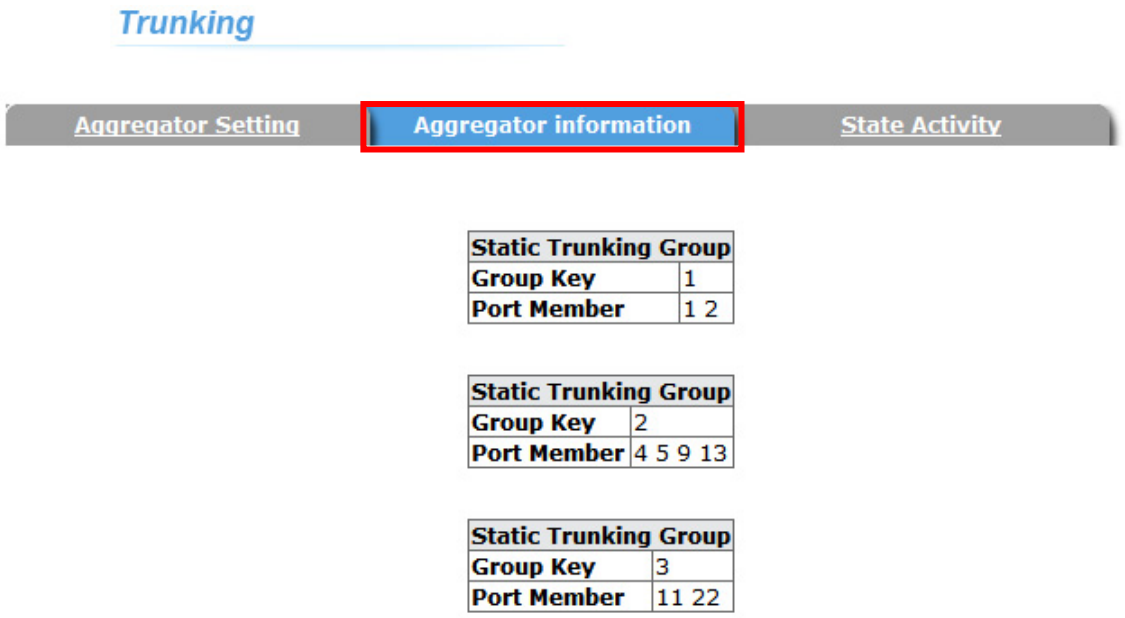
4.4.5.2 Aggregator Information

When you had setup the aggregator with LACP disabled, you will see related information in here.

Group Key: It shows your Group ID.

Port member: It show which ports are in this Group Key.

In below figure, it shows that you have configured three Trunking groups, Group 1 has member port 1 and 2; Group 2 has member port 4, 5, 9 and 13; Group 3 has member port 11 and 22.



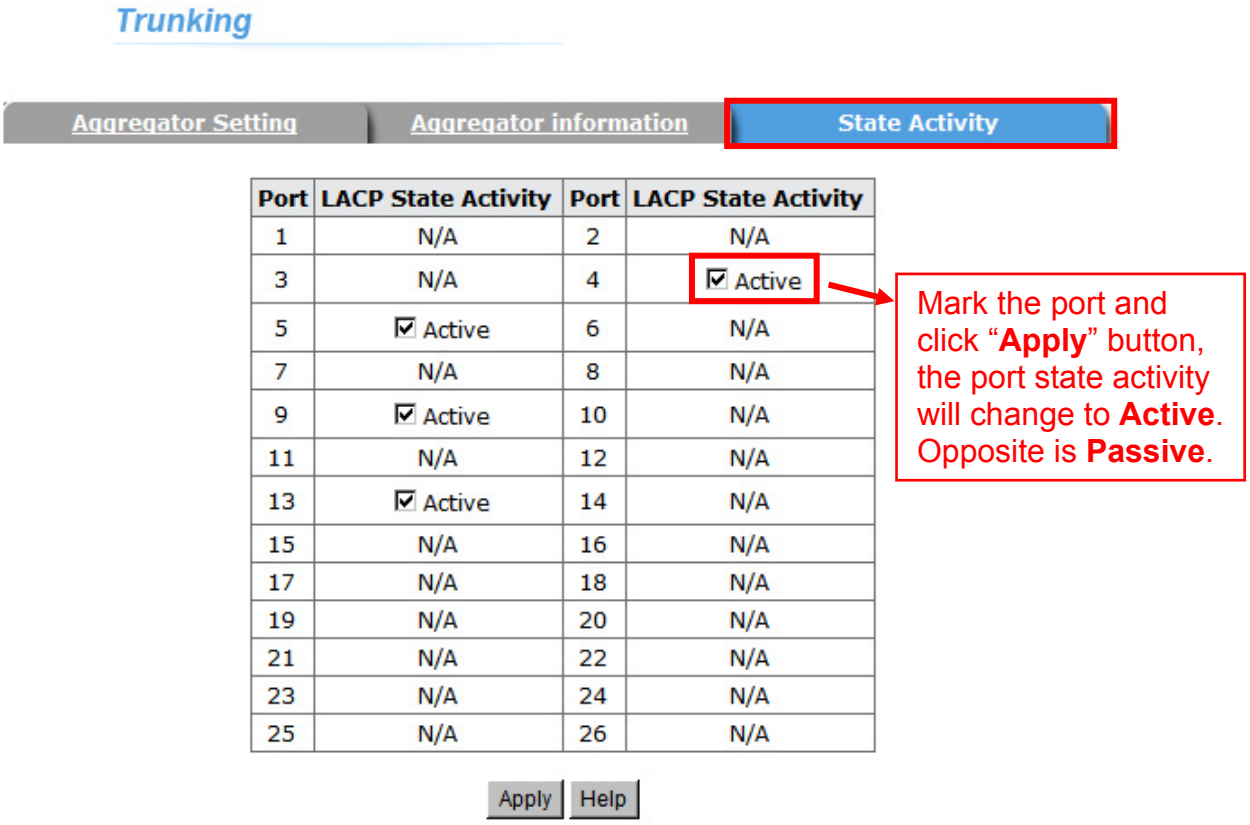
4.4.5.3 State Activity

When setup the LACP aggregator, you can configure port state activity. You can mark or un-mark the port. When you mark the port and click "**Apply**" button, the port state activity will change to **Active**. Opposite is **Passive**.

1. **Active:** The port automatically sends LACP protocol packets.
2. **Passive:** The port does not automatically send LACP protocol packets, and responds only if it receives LACP protocol packets from the opposite device.

Note:

- A link having either two active LACP ports or one active port can perform dynamic LACP trunking.
- A link having two passive LACP ports will not perform dynamic LACP trunking because both ports are waiting for LACP protocol packet from the opposite device.
- If you are active LACP's actor, when you are selecting trunking port, the active status will be created automatically.



4.4.6 Forwarding and Filtering

The Internet Group Management Protocol (IGMP) is an internal protocol of the Internet Protocol (IP) suite. IP manages multicast traffic by using switches, routers, and hosts that support IGMP. Enabling IGMP allows the ports to detect IGMP queries and report packets and manage IP multicast traffic through the switch.

4.4.6.1 IGMP Snooping

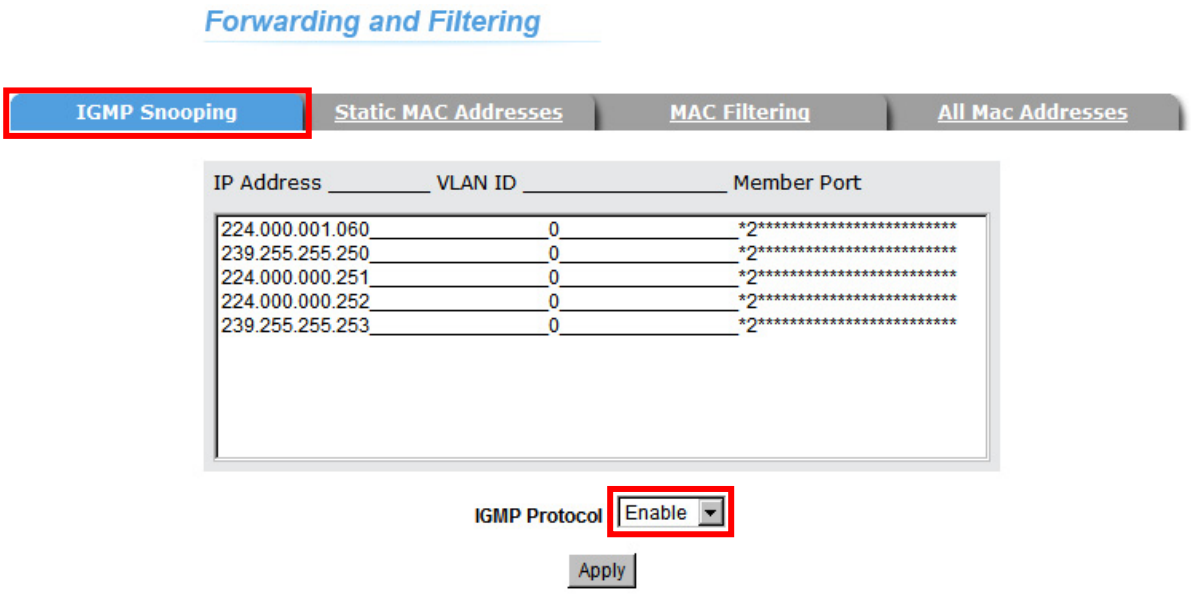
IGMP snooping is designed to prevent hosts on a local network from receiving traffic for a multicast group they have not explicitly joined. It provides switches with a mechanism to prune multicast traffic from links that do not contain a multicast listener (IGMP client). A switch which does not IGMP snooping will, by default, 'flood' multicast traffic to all the ports in a broadcast domain (or the VLAN equivalent). Multicast can cause unnecessary or even crippling load on host devices by requiring them to process packets they have not solicited.

The Switch supports IP multicast, you can enable IGMP protocol, and then display the IGMP snooping information in this page, you can view different multicast group VID and member port in here, and IP multicast addresses range from 224.0.0.0 through

239.255.255.255. IGMP have three fundamental types of message as follows:

Message	Description
Query	A message sent from the querier (IGMP router or switch) asking for a response from each host belonging to the multicast group.
Report	A message sent by a host to the querier to indicate that the host wants to be or is a member of a given group indicated in the report message.
Leave Group	A message sent by a host to the querier to indicate that the host has quited to be a member of a specific multicast group.

When you enable IGMP Query (refer to 4.2.2.3) and IGMP Snooping, you will see the related information showed as below figure.



4.4.6.2 Static MAC Address

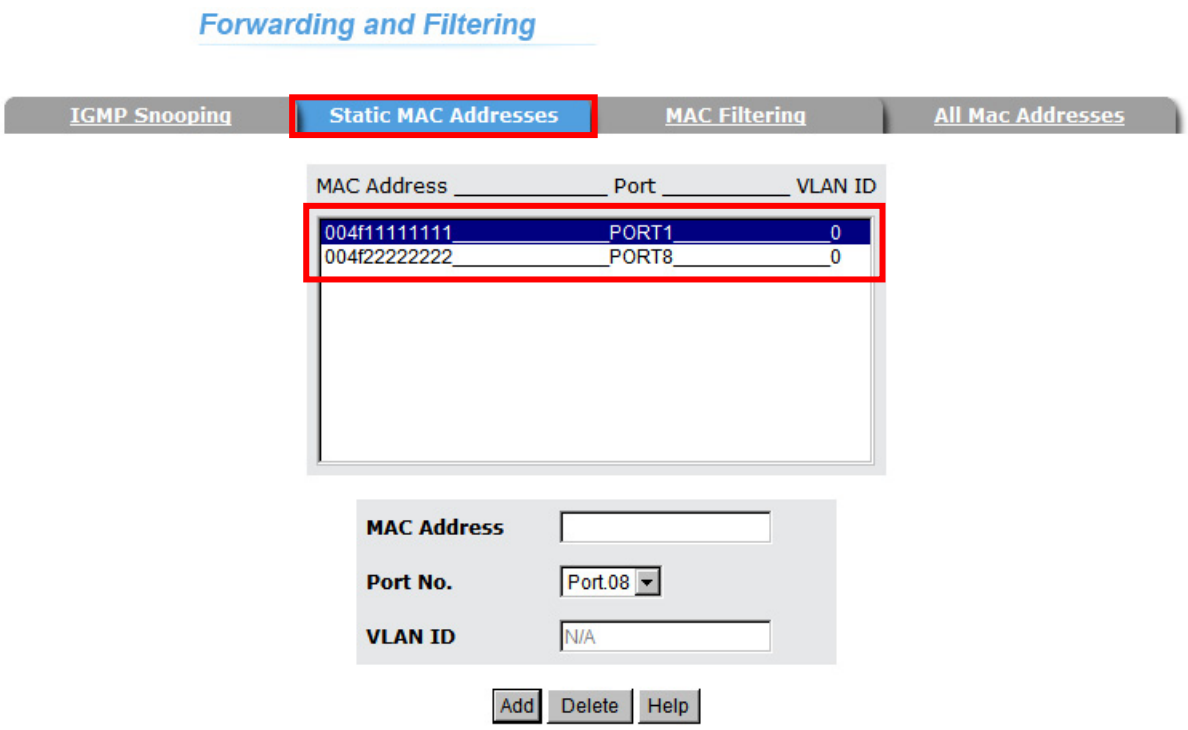
When you add a static MAC address, it remains in the switch's address table, regardless of whether the device is physically connected to the switch. This saves the switch from having to re-learn a device's MAC address when the disconnected or powered-off device is active on the network again.

1. In **MAC Address** column, enter the MAC address to and from which the port should

permanently forward traffic, regardless of the device network activity.

2. In the **Port No.** box, select a port number.
3. **VLAN ID:** If tag-based (IEEE 802.1Q) VLANs are set up on the switch, static addresses are associated with individual VLANs. Type the VID (tag-based VLANs) to associate with the MAC address.
4. Click "**Apply**" button to apply your setting
5. If user wants to delete one MAC address, please click the MAC address which you want to delete on the MAC address column, and then click "**Delete**" button to delete it.

In the below figure, it shows that you have created two static MAC address in the Switch. They are 004f11111111 on port 1 without VLAN ID and 004f22222222 on port 8 without VLAN ID, respectively.



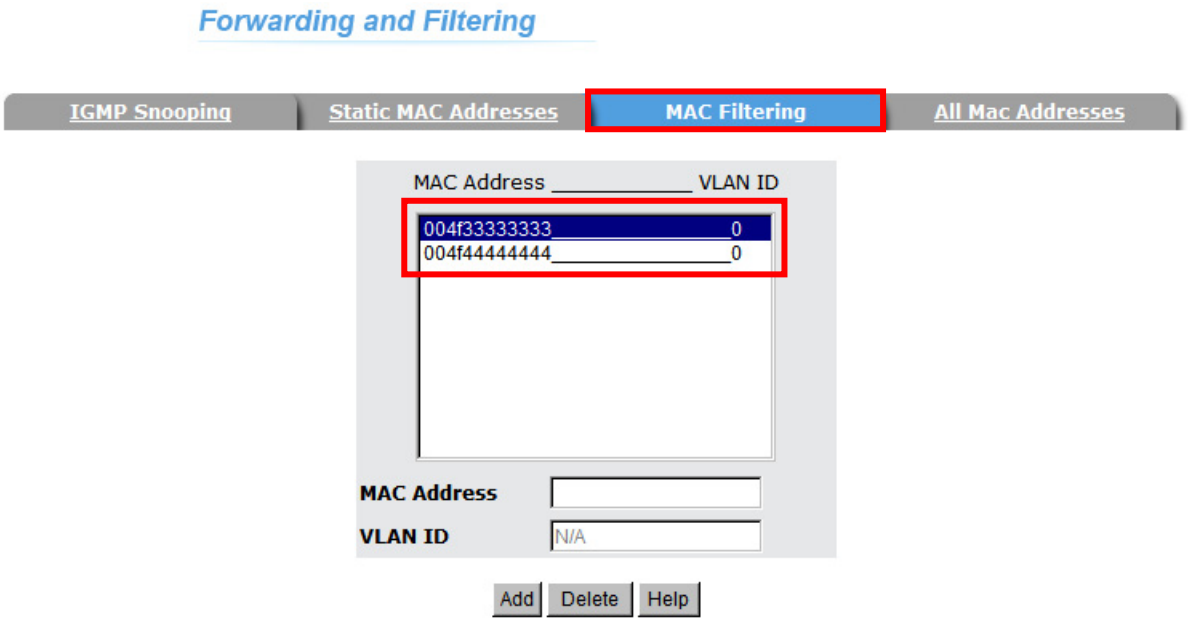
4.4.6.3 MAC filtering

MAC filtering function allows the switch to drop unwanted traffic. Traffic is filtered based on the destination MAC addresses.

1. In **MAC Address** box, enter the MAC address that wants to filter.
2. **VLAN ID:** If tag-based (802.1Q) VLAN are set up on the switch, type the VLAN ID in the box to associate with the MAC address.

3. Click “**Add**” button.
4. If user wants to delete one MAC address, please click the MAC address which you want to delete on the MAC address column, and then click “**Delete**” button to delete it.

In the below figure, it shows that you have created two MAC addresses that you want to filter in the switch. They are 004f33333333 without VLAN ID and 004f44444444 without VLAN ID, respectively.

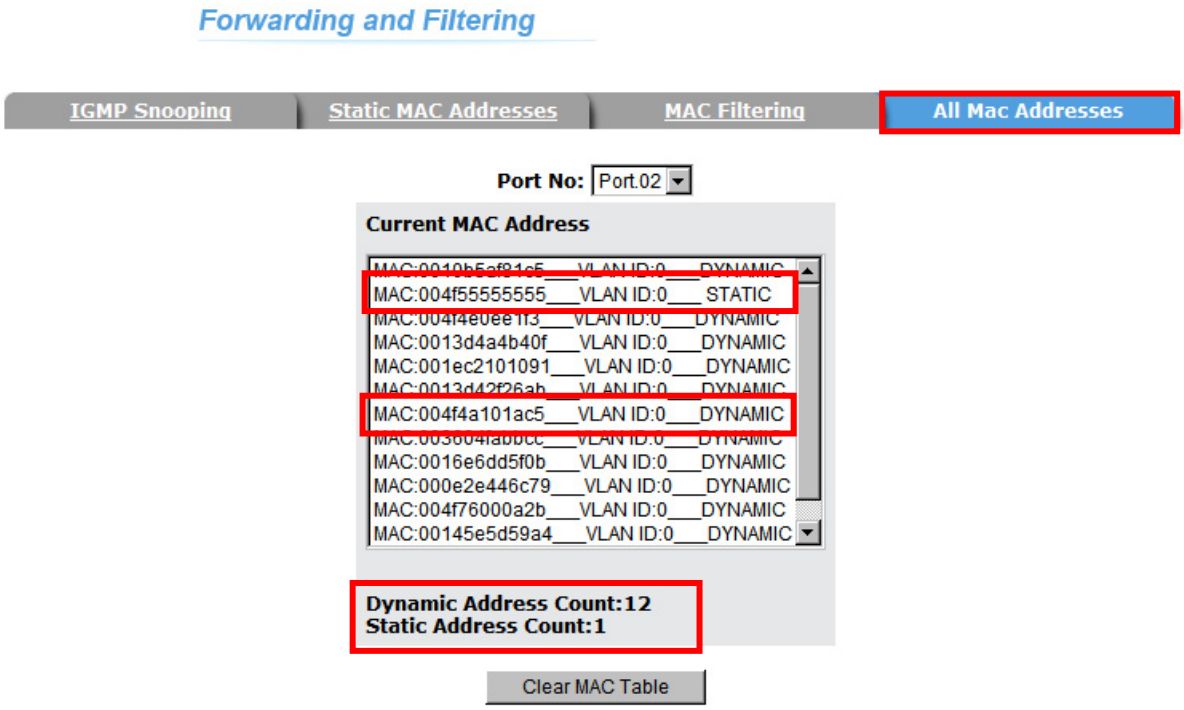


4.4.6.4 All MAC Addresses

You can view the port that connected device’s MAC address and the related devices’ MAC address.

1. Select the port.
2. The current static & dynamic MAC address information of the port will be displayed in here.
3. You also can click “Clear MAC Table” to clear the current MAC address information of the port on screen.

In the below figure, it shows that port 2 has record 12 dynamic MAC addresses and 1 static MAC addresses on MAC table.



4.4.7 VLAN configuration

A Virtual LAN (VLAN) is a logical network grouping that limits the broadcast domain. It allows you to isolate network traffic so only members of the VLAN receive traffic from the same VLAN members. Basically, creating a VLAN from a switch is logically equivalent of reconnecting a group of network devices to another Layer 2 switch. However, all the network devices are still plug into the same switch physically.

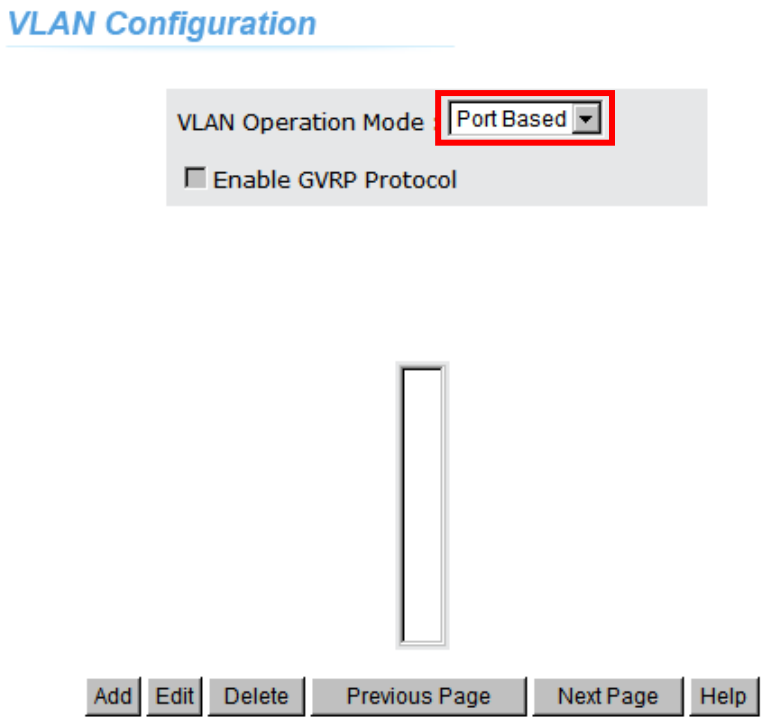
The switch supports port-based, 802.1Q (tagged-based) and protocol-base VLAN in web management page. In the default configuration, VLAN support is “disable”.

4.4.7.1 Port-based VLAN

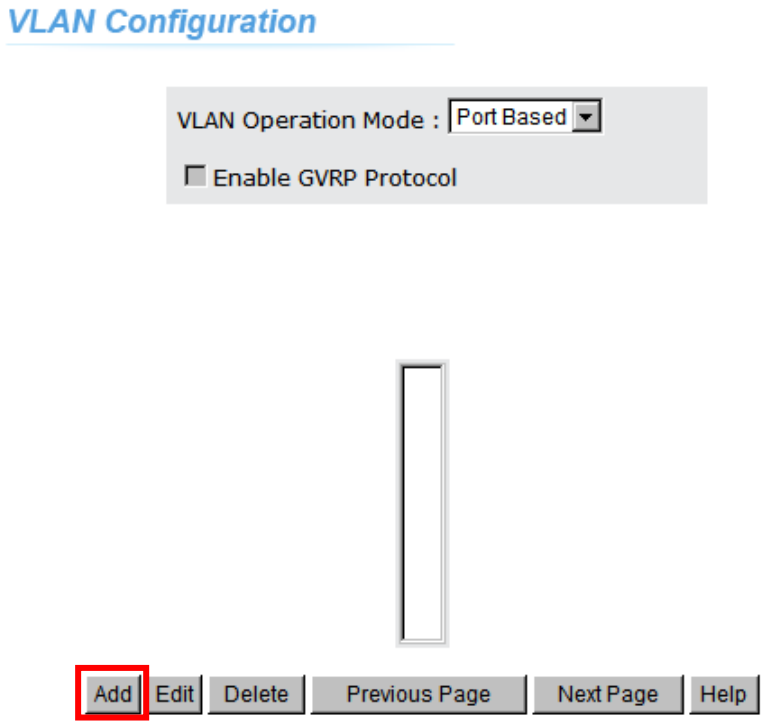
Packets can go among only members of the same VLAN group. Note all unselected ports are treated as belonging to another single VLAN. If the port-based VLAN enabled, the VLAN-tagging is ignored.

In order for an end station to send packets to different VLANs, it itself has to be either capable of tagging packets it sends with VLAN tags or attached to a VLAN-aware bridge

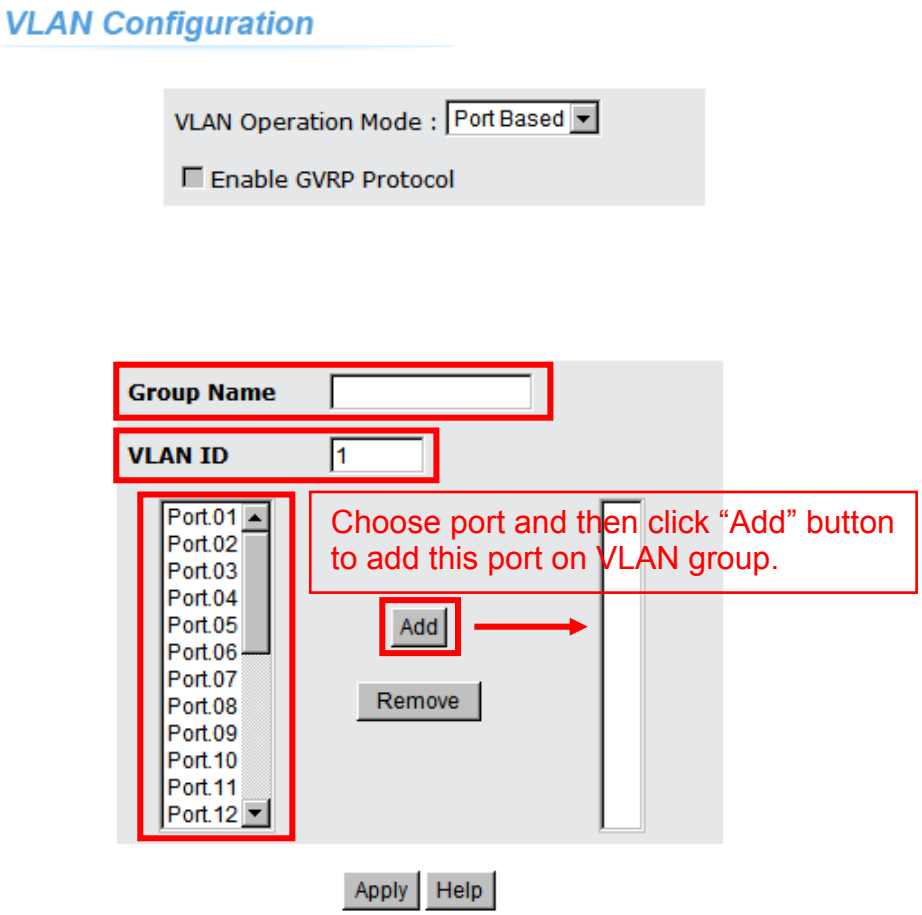
that is capable of classifying and tagging the packet with different VLAN ID based on not only default PVID but also other information about the packet, such as the protocol.



1. Click "**Add**" button, then below screen will display. You can create a new VLAN group.

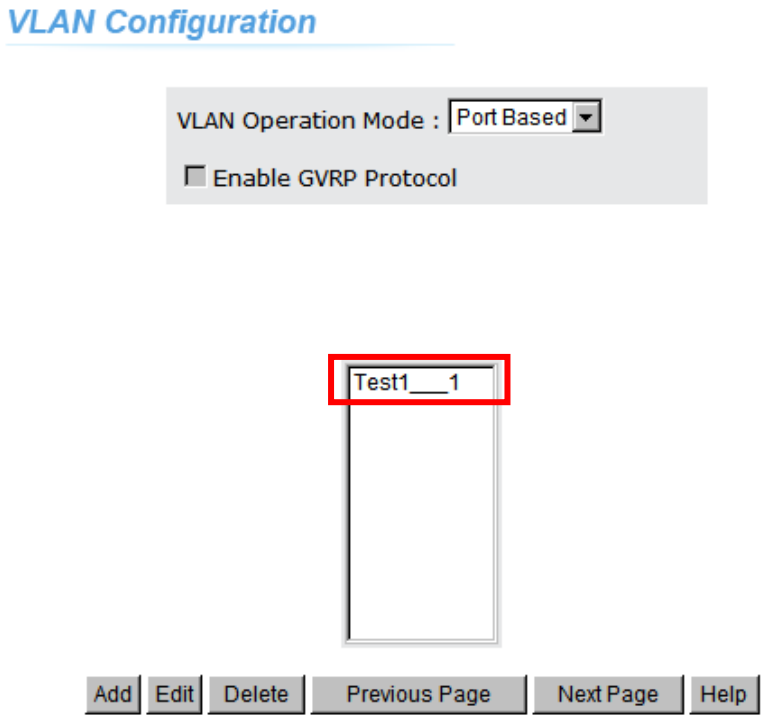


2. Enter the Group Name, VLAN ID and select the members of VLAN group, then click "**Add**" button to add members to right column.



3. Click "**Apply**" button to apply your setting.
4. After creating one VLAN, you will see the VLAN group displays in main screen.

   In the below figure, it show that you have created one VLAN group whose Group name is Test1 and VLAN ID is 1.



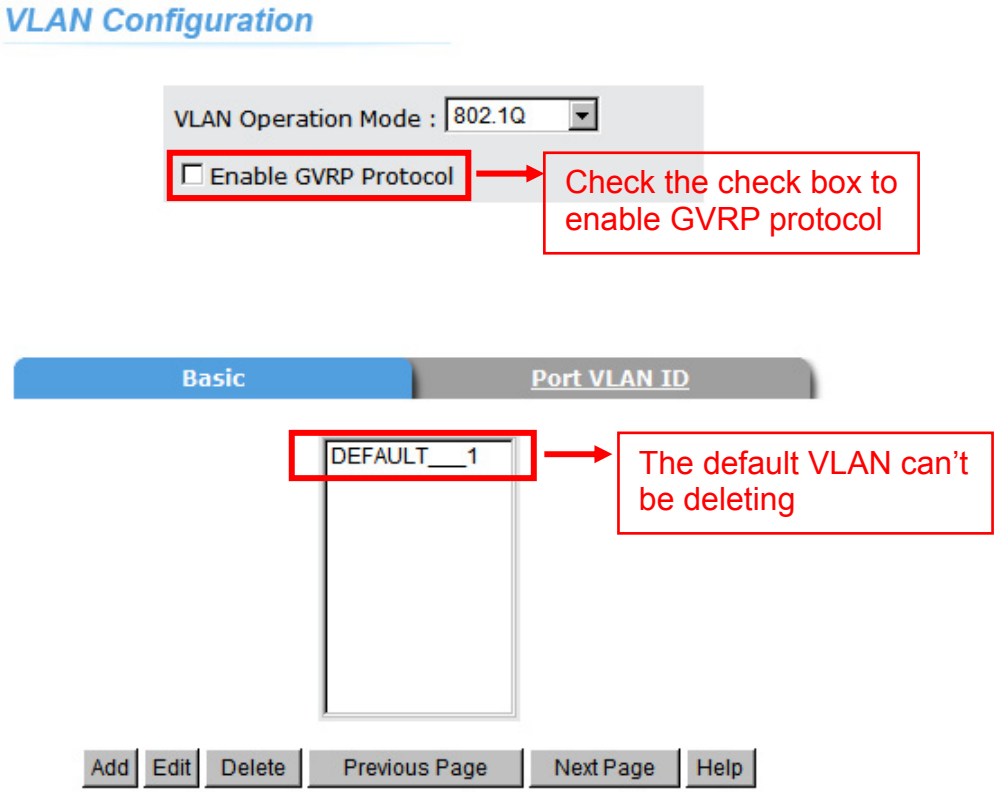
5. If the group's list is over one page, you can click "**Next Page**" button to view other VLAN groups.
6. Use "**Delete**" button to delete unwanted VLAN.
7. Use "**Edit**" button to modify existing VLAN group.

4.4.7.2 802.1Q VLAN

Tagged-based VLAN is an IEEE 802.1Q specification standard. Therefore, it is possible to create a VLAN across devices from different switch venders. IEEE 802.1Q VLAN uses a technique to insert a "tag" into the Ethernet frames. Tag contains a VLAN Identifier (VID) that indicates the VLAN numbers.

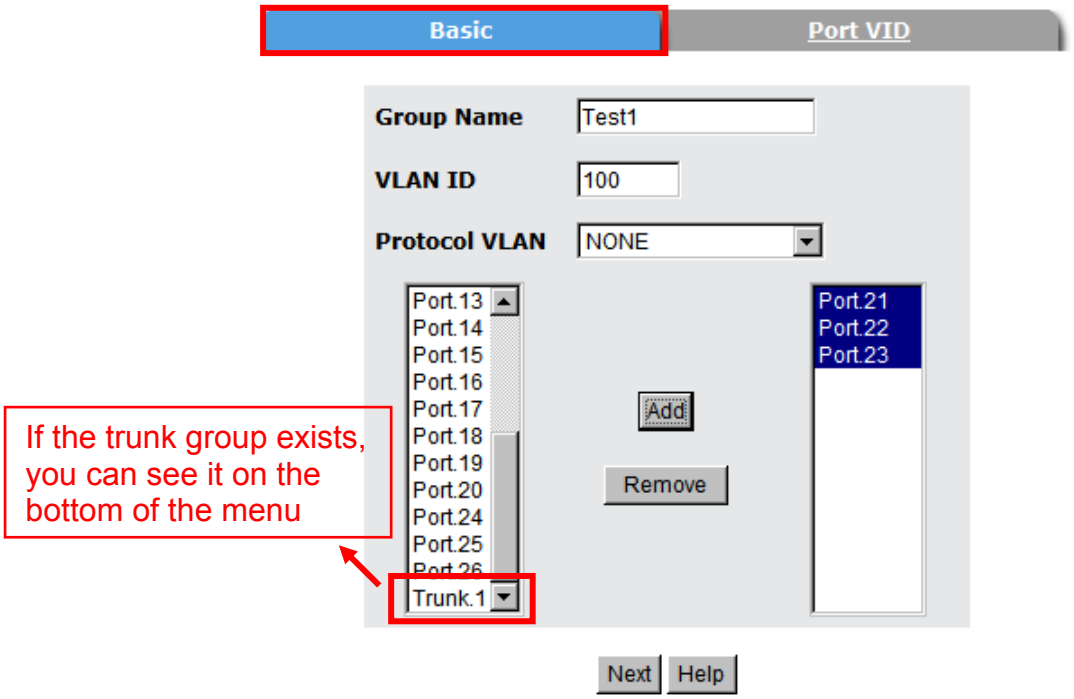
You can create Tag-based VLAN, and enable or disable GVRP protocol. There are 256 VLAN groups provided to configure. Enable 802.1Q VLAN, the all ports on the switch belong to default VLAN, VID is 1. The default VLAN can't be deleting.

GVRP allows automatic VLAN configuration between the switch and nodes. If the switch is connected to a device with GVRP enabled, you can send a GVRP request using the VID of a VLAN defined on the switch; the switch will automatically add that device to the existing VLAN.

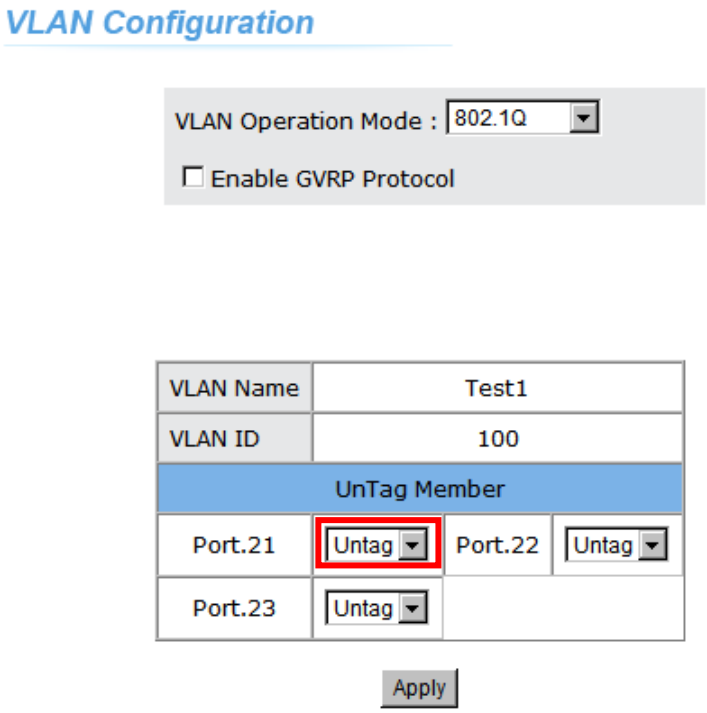


Basic

1. Click "**Add**" button to create new VLAN.
2. Group Name: Assign a name for new VLAN.
3. **Enable GVRP Protocol**: Check the check box to enable GVRP protocol.
4. **VLAN ID**: Fill in a VLAN ID (between 2 to 4094). The default is 1.
5. **Protocol VLAN:** Choose the protocol type. Default is NONE.
6. From the available port box, select ports to add to the switch and click "**Add**" button. If the trunk group exists, you can see it on the bottom of the menu (ex: Trunk. 1), and you can configure it as the member of the VLAN or not.



7. Click "**Next**" button, then you will see the page as below



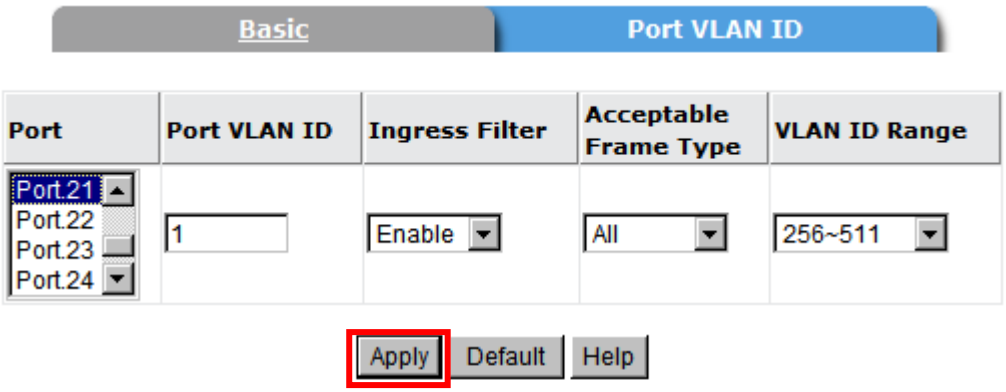
8. To set the outgoing frames are VLAN-Tagged frames or untagged. Then click "**Apply**" button to apply your setting.
   - Tag: outgoing frames with VLAN-Tagged.

- Untag: outgoing frames without VLAN-Tagged.

Port VID

In this page, you can configure port VID setting.

1. **Port VLAN ID**: Enter the port VLAN ID
2. **Ingress Filtering:** Ingress filtering lets frames belonging to a specific VLAN to be forwarded if the port belongs to that VLAN.
   - **Enable**: Forward only packets with VID matching this port's configured VID.
   - **Disable**: Disable Ingress filter function
3. **Acceptable Frame type:**
   - **Tag Only:** Only packet with match VLAN ID can be permission to go through the port.
   - **ALL:** Acceptable all Packet
4. **VLAN ID Range:** Select a range of VLAN ID. There are 16 VLAN ID range. The ports are assigned to the same VLAN ID will be in the same VLAN group.
5. Click "**Apply**" button to apply your setting.
6. To reset back to default value, click "**Default**" button.



Port	Port VLAN ID	Ingress Filter	Acceptable Frame Type
Port.21	1	Enable	All

4.4.8 Spanning Tree

The Spanning Tree Protocol (STP) is a network protocol that ensures a loop-free topology for any bridged LAN. Spanning tree allows a network design to include spare (redundant) links to provide automatic backup paths if an active link fails, without the danger of bridge loops, or the need for manual enabling/disabling of these backup links. Bridge loops must be avoided because they result in flooding the network.

Rapid Spanning Tree Protocol (RSTP), which provides for faster spanning tree convergence after a topology change. STP can take 30 to 50 seconds to respond to a topology change, RSTP is typically able to respond to changes within a second.

Basic spanning protocol will follow the below rules:

1. **Select a root bridge**: The root bridge of the spanning tree is the bridge with the smallest bridge ID. Every bridge has a unique ID and a configurable priority number; the bridge ID contains both numbers. To compare two bridge IDs, the priority is compared first. If two bridges have equal priority, then the MAC addresses are compared. For example, if switches A (MAC=000000001111) and B (MAC=000000002222) both have a priority of 10, then switch A will be selected as the root bridge because of smaller MAC address.
2. **Determine the least cost paths to the root bridge**: The lease cost path is a path from the device to the root that has minimum cost among all paths from the device to the root.
3. **Disable all other root paths**: Any active port that is not a root port or a designated port is a blocked port.
4. **Modification in case of ties**: In some sophisticated network, two or more ports on a single bridge are attached to least-cost paths to the root or two or more bridges on the same network segment have equal least-cost paths to the root. They are so-called ties, Spanning tree protocol would break such ties for better usage.

System Configuration

1. You can view spanning tree status about the switch.
2. You can modify RSTP state. After modifying, click “**Apply**” button to apply your setting.
3. **RSTP Mode:** Select “Disable”, “802.1d (STP)” or “802.1w (RSTP)”. The default is “Disabled”.
4. Once selecting 802.1d or 802.1w, you can configure the below setting.
   - **Priority:** Assign path priority number. The valid value is from 0 to 61440. The default is 32678.
   - **Max Age:** When the SNMP-FSH2602MG v2 is the root bridge, the whole LAN will apply this figure set by this switch as their maximum age time. When a bridge received a BPDU originated from the root bridge and if the message age conveyed in the BPDU exceeds the Max. Age of the root bridge, the bridge will

treat the root bridge malfunctioned and issue a Topology Change Notification (TCN) BPDU to all other bridges. All bridges in the LAN will re-calculate and determine who the root bridge is. The valid value is from 6 to 40 seconds. The default is 20 seconds.

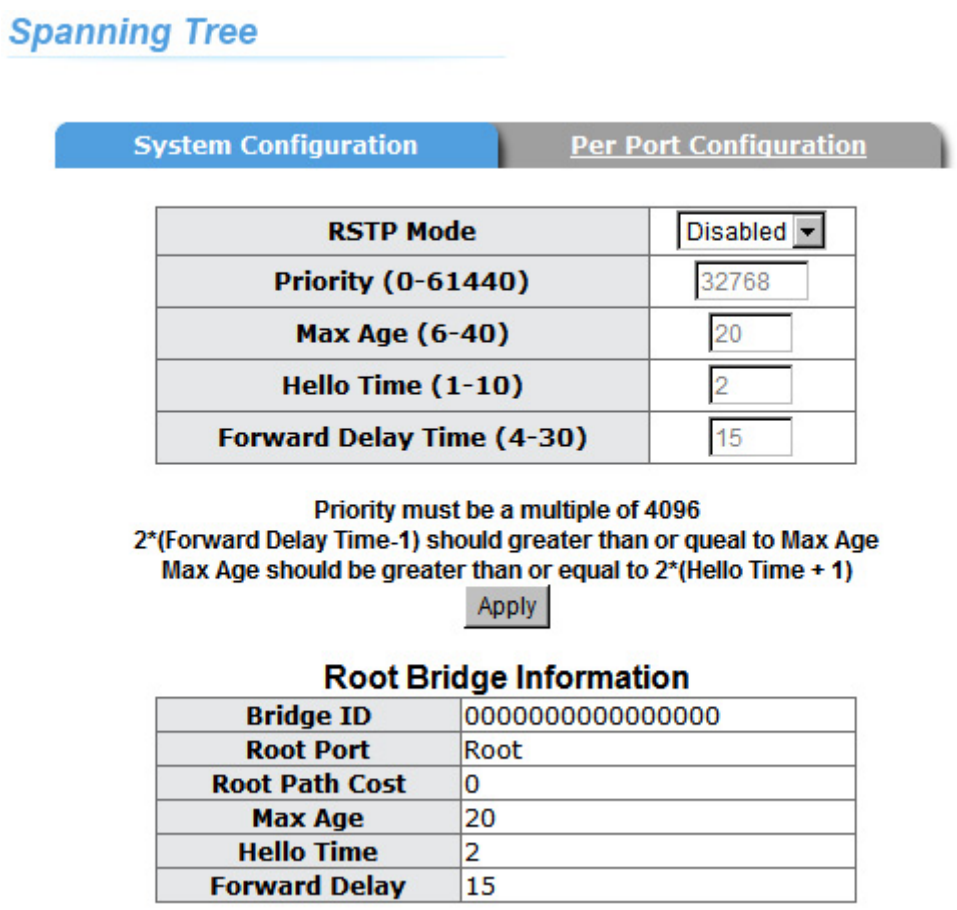
- **Hello Time:** The time that how long a switch sends BPDU packet to other bridge checks STP current status. The valid value is from 1 to 10 seconds. The default is 2 seconds.
- **Forward Delay Time:** The forward delay time is defined as the time spent from Listening state moved to Learning state and also from Learning state moved to Forwarding state of a port in bridge. The forward delay time contains two states, Listening state to Learning state and Learning state to Forwarding state. It assumes that forward delay time is 15 seconds, and total forward delay time will be 30 seconds. This has much to do with the STP convergent time which will be more than 30 seconds because some other factors. The valid value is from 4 to 30 seconds. The default is 45 seconds.

Note:

(1) Priority must be a multiple of 4096.

(2) 2 x (Forward Delay Time-1) should be greater than or equal to Max Age.

(3) Max Age should be greater than or equal to 2 x (Hello Time + 1).



Per Port Configuration

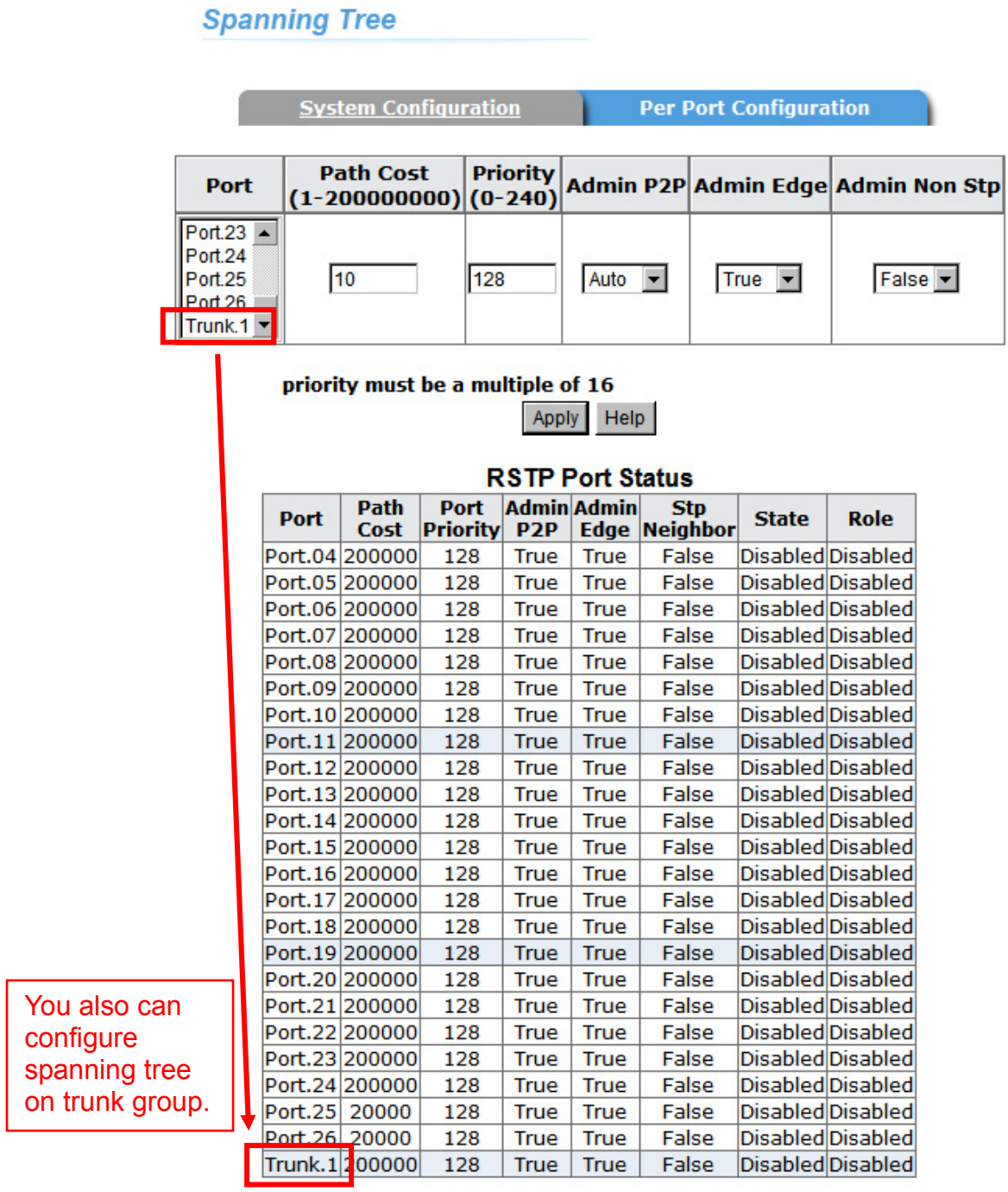
You can configure path cost and priority of every port.

1. Select the port in Port column.
2. Assign the **Path Cost**. It is the cost of the path to the other bridge from this transmitting bridge at the specified port. The value range is from 1 to 200000000. The default is 200000.
3. Assign the **port priority value**. It decides which port should be blocked by priority in LAN. The valid value is from 0 to 240. The lowest value has higher priority. The default is 128. Priority must be a multiple of 16.
4. Assign the **Admin P2P**. From RSTP's view, a port is a point-to-point link if it is in full-duplex mode but is shared link if it is in half-duplex mode. RSTP fast convergence can only happen on point-to-point links and on edge ports. This can expedite the convergence because this will have the port fast transited to forwarding state. There are three parameters, Auto, True and False, used to configure the type of the point-to-point link. If configuring this parameter to be Auto, it means RSTP will use the duplex mode resulted from the auto-negotiation. In today's switched networks, most links are running in full-duplex mode. For sure, the result may be half-duplex, in this case, the port will not fast transit to Forwarding state. If it is set as True, the port is treated as point-to-point link by RSTP and unconditionally transited to Forwarding state. If it is set as False, fast transition to Forwarding state will not happen on this port. The default is Auto.
5. Assign the **Admin Edge**. If user selects "True", this port will be an edge port. An Edge Port is a port connected to a device that knows nothing about STP or RSTP. Usually, the connected device is an end station. Edge Ports will immediately transit to forwarding state and skip the listening and learning state because the edge ports cannot create bridging loops in the network. This will expedite the convergence. When the link on the edge port toggles, the STP topology keeps unchanged. Unlike the designate port or root port though, an edge port will transit to a normal spanning-tree port immediately if it receives a BPDU. The default is True.
6. Assign the **Admin Non Stp**. The port includes the STP mathematic calculation. True is not including STP mathematic calculation. False is including the STP mathematic calculation. The default is False.
7. Click "**Apply**" button to apply your setting.

Note: If the trunk group exists, you can see it in port menu (ex: Trunk. 1), and you also can configure it for spanning tree configuration.

.

User can view the RSTP port status showed in bottom of webpage. It will display the status of every port.


Spanning Tree
System Configuration
Per Port Configuration
Port
Path Cost (1-200000000)
Priority (0-240)
Admin P2P
Admin Edge
Admin Non Stp
Port.23
Port.24
Port.25
Port.26
Trunk.1
10
128
Auto
True
False
priority must be a multiple of 16
Apply
Help
RSTP Port Status
Port
Path Cost
Port Priority
Admin P2P
Admin Edge
Stp Neighbor
State
Role
Port.04 200000 128 True True False Disabled Disabled
Port.05 200000 128 True True False Disabled Disabled
Port.06 200000 128 True True False Disabled Disabled
Port.07 200000 128 True True False Disabled Disabled
Port.08 200000 128 True True False Disabled Disabled
Port.09 200000 128 True True False Disabled Disabled
Port.10 200000 128 True True False Disabled Disabled
Port.11 200000 128 True True False Disabled Disabled
Port.12 200000 128 True True False Disabled Disabled
Port.13 200000 128 True True False Disabled Disabled
Port.14 200000 128 True True False Disabled Disabled
Port.15 200000 128 True True False Disabled Disabled
Port.16 200000 128 True True False Disabled Disabled
Port.17 200000 128 True True False Disabled Disabled
Port.18 200000 128 True True False Disabled Disabled
Port.19 200000 128 True True False Disabled Disabled
Port.20 200000 128 True True False Disabled Disabled
Port.21 200000 128 True True False Disabled Disabled
Port.22 200000 128 True True False Disabled Disabled
Port.23 200000 128 True True False Disabled Disabled
Port.24 200000 128 True True False Disabled Disabled
Port.25 20000 128 True True False Disabled Disabled
Port.26 20000 128 True True False Disabled Disabled
Trunk.1 200000 128 True True False Disabled Disabled
You also can configure spanning tree on trunk group.

4.4.9 Port Mirroring

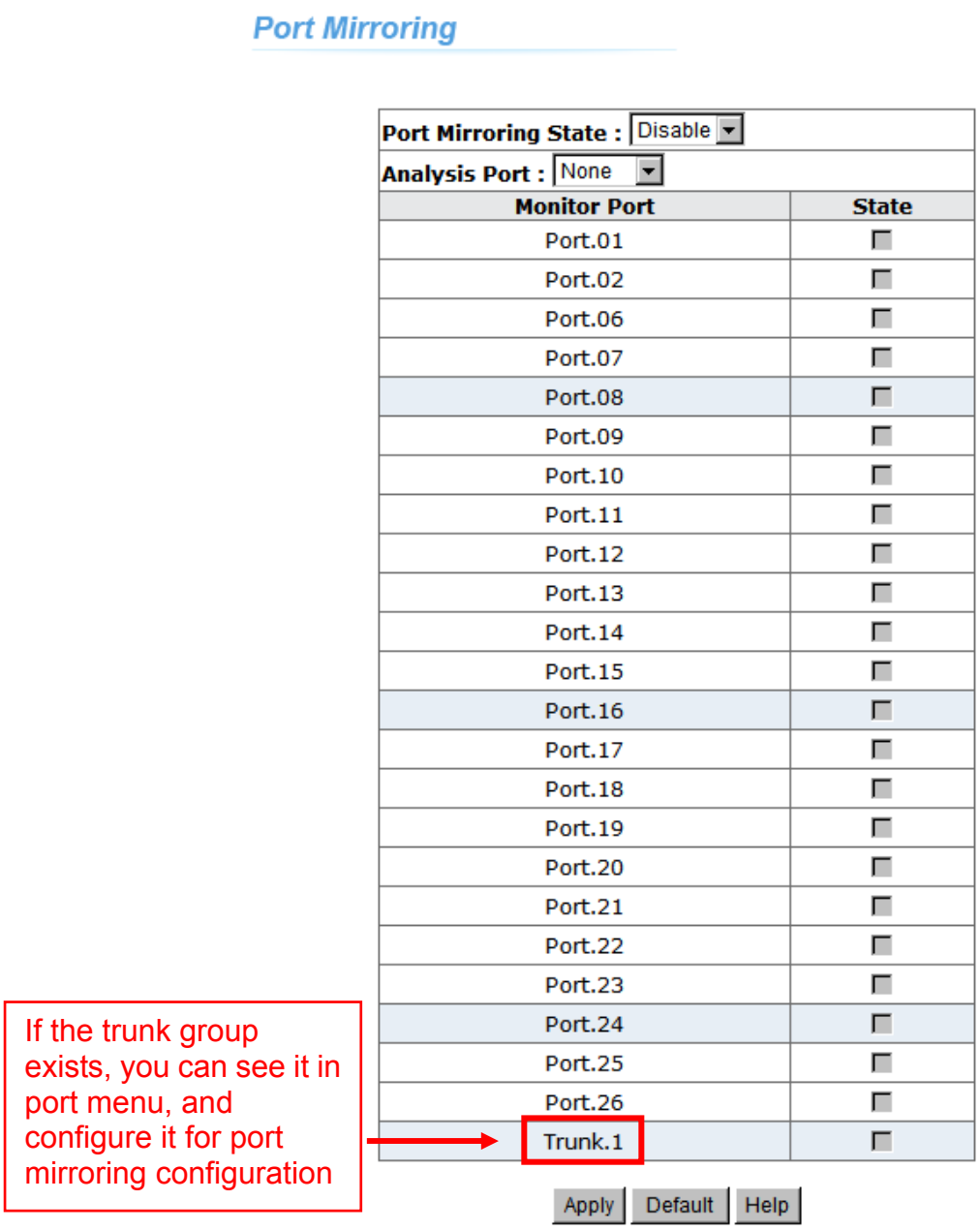
The Port mirroring is a method for monitoring traffic in switched networks. Traffic through ports can be monitored by one specific port. That is, traffic goes in or out monitored ports will be duplicated into mirror port.

1. **Port Mirroring State:** User can select “Disable”, “RX”, “TX”, and “Both”.

2. **Analysis Port:** It means mirror port can be used to see all monitored port traffic. You can connect mirror port to LAN analyzer or Netxray.
3. **Monitor Port:** The ports you want to monitor. All monitored port traffic will be copied to mirror port. You can select max 25 monitor ports in the switch. User can choose which port wants to monitor in only one mirror mode.

Note:

- If you want to disable the function, you must select monitor port to none.
- If the trunk group exists, you can see it in port menu (ex: Trunk. 1), and you also can configure it for port mirroring configuration



4.4.10 SNMP Management

The SNMP (Simple Network Management Protocol) is a Protocol that governs the transfer of information between management and agent. The switch supports SNMP V1.

You can define management stations as trap managers and to enter SNMP community strings. You also can define a name, location, and contact person for the switch. Fill in the system options data, and then click ”**Apply**” button to update the changes.

(1) System Options

- **Name:** Enter a name for the switch.
- **Location:** Enter the switch’s physical location.
- **Contact:** Enter the name of contact person or organization.

After entering the above information, please click “**Apply**” button to apply your setting.

(2) Community strings

Serve as a password between trap manager and switch.

- **String:** Fill the name of string.
- **RO:** Read only. Enable requests accompanied by this string to display MIB-object information.
- **RW:** Read write. Enable requests accompanied by this string to display MIB-object information and to set MIB objects.

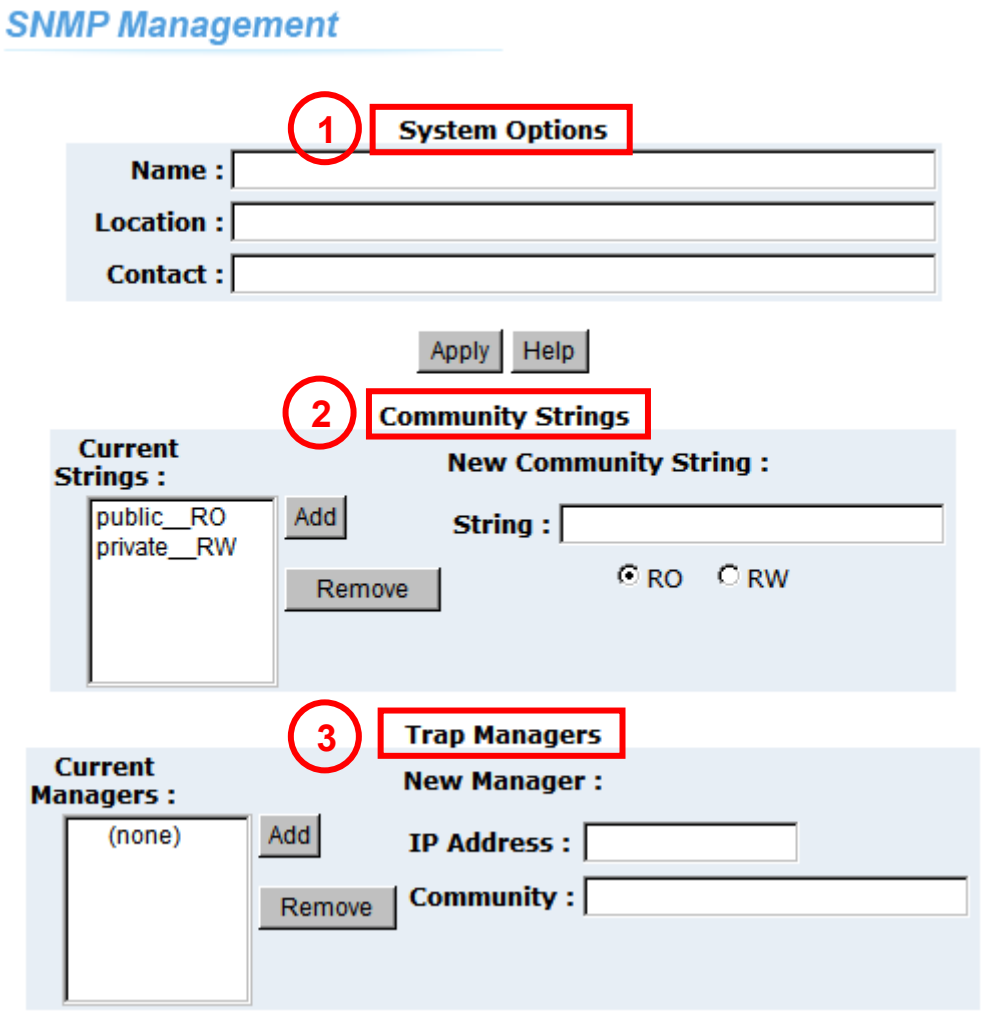
Once entering the above information, please click “**Add**” button to add your new string. If you want to remove one string, please click “**Remove**” button to remove the string.

(3) Trap Manager

A trap manager is a management station that receives traps, the system alerts generated by the switch. If no trap manager is defined, no traps will issue. Create a trap manager by entering the IP address of the station and a community string.

- **IP Address:** fill in the trap device IP.
- **Community Strings:** the trap device community strings.

After entering the above information, please click “**Add**” button to add your new Trap Manager. If you want to remove one Trap Manager, please click “**Remove**” button to remove the Trap Manager.

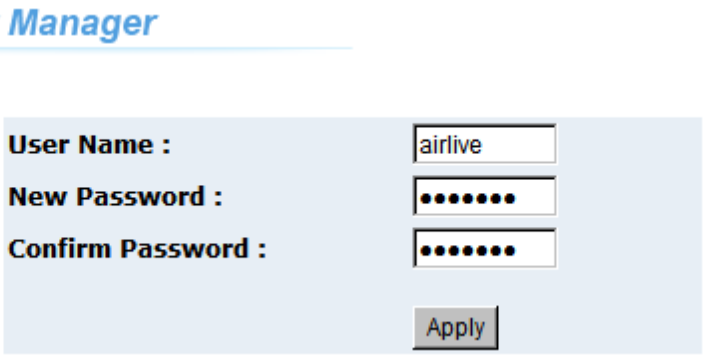


4.4.11 Security Manager

You can change web management login user name and password.

- **User name:** Type the new user name. The default is "**airlive**"
- **Password:** Type the new password. The default is "**airlive**"
- **Confirm password:** Re-type the new password to confirm your new password.

After changing the above information, please click "**Apply**" button to apply your setting.

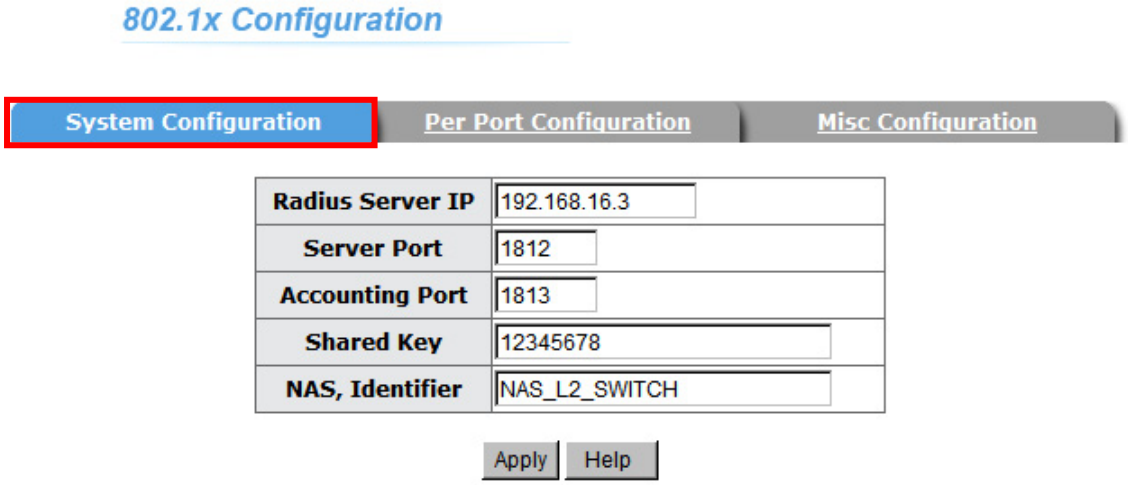


4.4.12 802.1X

When enabling the IEEE 802.1X function, you can configure the parameters of this function.

System Configuration

1. **Radius Server IP:** Set the IP address of Radius Server.
2. **Server Port:** Set the UDP destination port for authentication requests to the specified Radius Server.
3. **Accounting Port:** Set the UDP destination port for accounting requests to the specified Radius Server.
4. **Shared Key:** Set an encryption key for use during authentication sessions with the specified radius server. This key must match the encryption key used on the Radius Server.
5. **NAS, Identifier:** Set the identifier for the radius client.
6. Click "**Apply**" button to apply your setting.

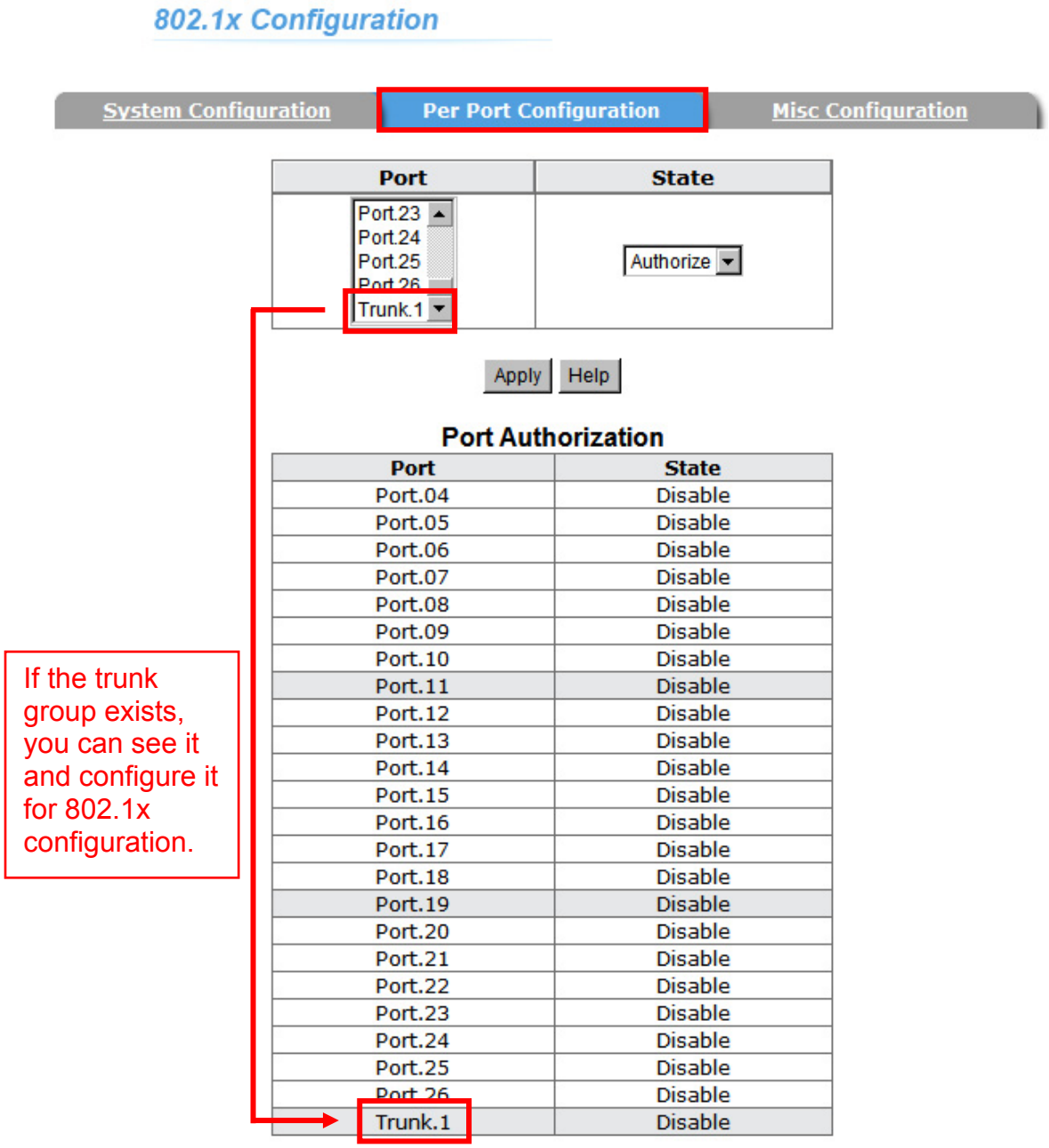


Per Port Configuration

1. Select the port in Port column.
2. Select the state of port. There are four states:
   - **Reject:** The specified port is forced to be held in the Unauthorized state.
   - **Accept:** The specified port is forced to be held in the Authorized state.
   - **Authorized:** The specified port is set to the Authorized or Unauthorized state in accordance with the outcome of an authentication exchange between the Supplicant and the authentication server.
   - **Disable:** The specified port did not support 802.1x function.
3. Click "**Apply**" button to apply your setting.

You can see the every port Authorization information listed in table.

Note: If the trunk group exists, you can see it in port menu (ex: Trunk. 1), and you also can configure it for 802.1x configuration.

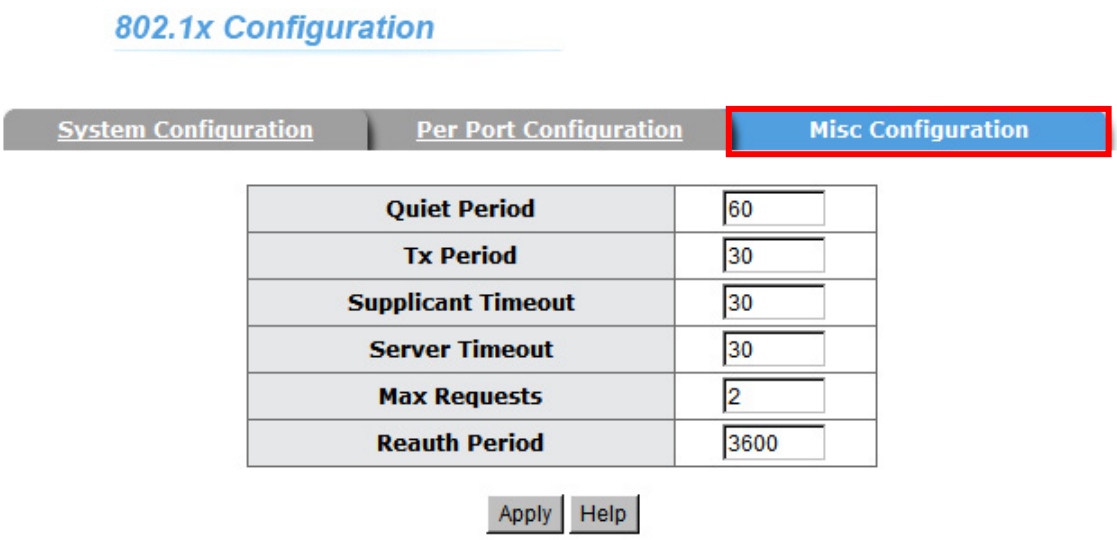


Misc Configuration

1. **Quiet period:** Set the period during which the port doesn't try to acquire a supplicant. The valid range is 1 to 65535. The default time is 60 seconds.
2. **TX period:** Set the period the port waits to re-transmit next EAPOL PDU during an authentication session. The valid range is from 1 to 65535. The default time is 30 seconds.
3. **Supplicant timeout:** Set the period of time the switch waits for a supplicant response

to an EAP request. The valid range is from 1 to 300. The default time is 30 seconds.

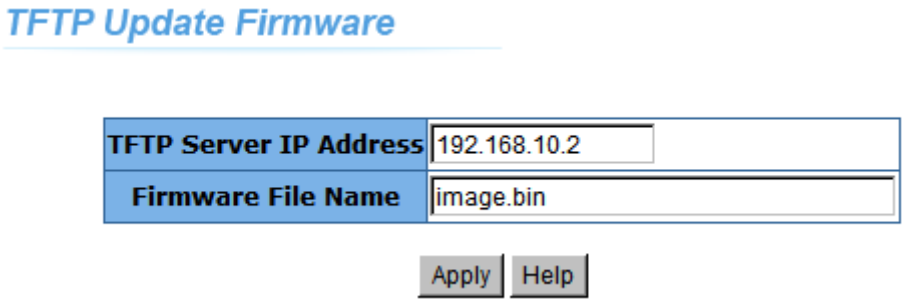
4. **Server timeout:** Set the period of time the switch waits for a server response to an authentication request. The valid range is from 1 to 300. The default time is 30 seconds
5. **Max requests:** Set the number of authentication that must time-out before authentication fails and the authentication session ends. The valid range is from 1 to 10. The default value is 2 times.
6. **Reauth period:** Set the period of time after which clients connected must be re-authenticated. The valid range is from 1 to 99999. The default value is 3600 seconds.



4.5 TFTP Update Firmware

It provides the functions to allow a user to update the switch firmware. Before updating, make sure you have your TFTP server ready and the firmware image is on the TFTP server.

1. **TFTP Server IP Address:** Fill in your TFTP server IP. The default IP address is 192.168.10.2.
2. **Firmware File Name:** Fill the name of firmware image. The default file name is image.bin.
3. Click "**Apply**" button to upgrade the firmware.



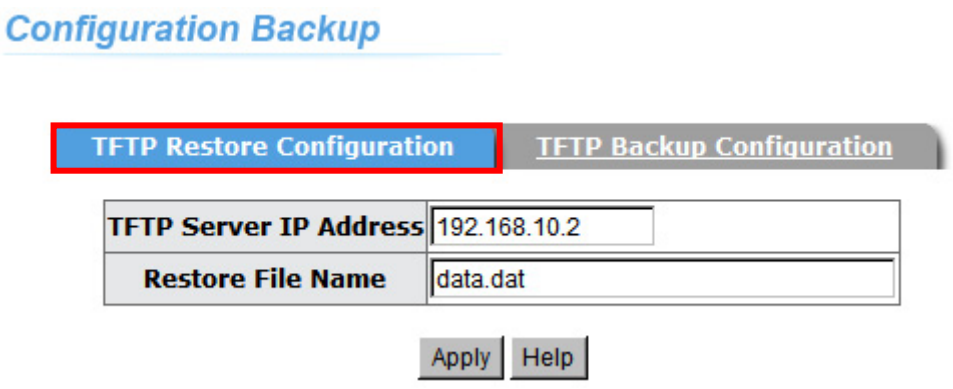
4.6 Configuration Backup

In Configuration Backup, you can restore the backup configuration into the switch. Also, you can backup the configuration to TFTP server.

TFTP Restore Configuration

You can restore EEPROM value from TFTP server, but you must put back image in TFTP server, switch will download back flash image.

1. **TFTP Server IP Address:** fill in the TFTP server IP.
2. **Restore File Name:** fill in the correct restore file name.
3. Click "**Apply**" button to restore configuration file.

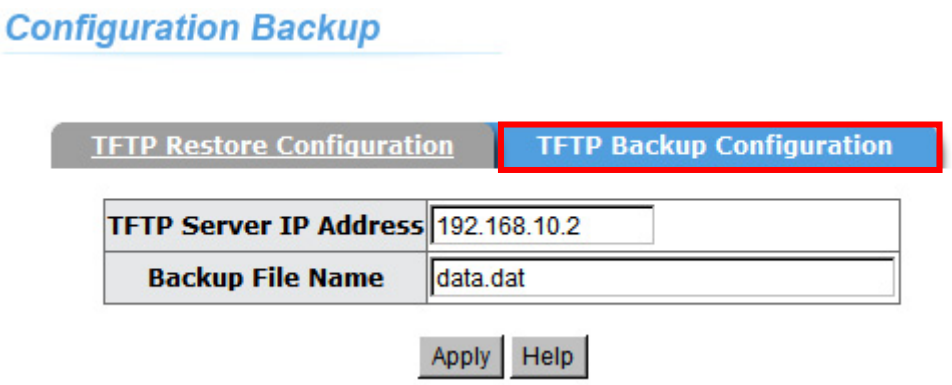


TFTP Backup Configuration

You can save current EEPROM value from the switch to TFTP server, then go to the TFTP

restore configuration page to restore the EEPROM value.

1. **TFTP Server IP Address:** Fill in the TFTP server IP. The default IP address is 192.168.10.2.
2. **Backup File Name:** Fill the file name. The default file name is image.bin.
3. Click "**Apply**" button to restore configuration file.

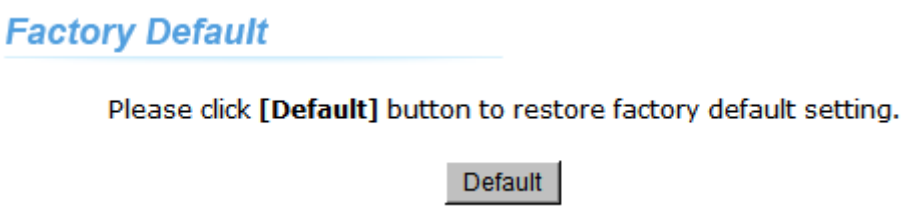


4.7 Factory Default

Reset Switch to default configuration, default value to as following configuration:

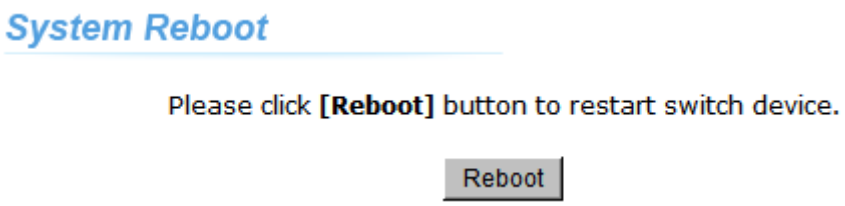
- **Default IP address:** 192.168.10.1
- **Default Gateway:** 192.168.10.254
- **Subnet mask:** 255.255.255.0
- The other setting value is back to disable or none.

Click "**Default**" button to reset switch to default setting. Once resetting to factory default successfully, Switch will ask user to reboot the Switch, please click "reboot" button to reboot the Switch.



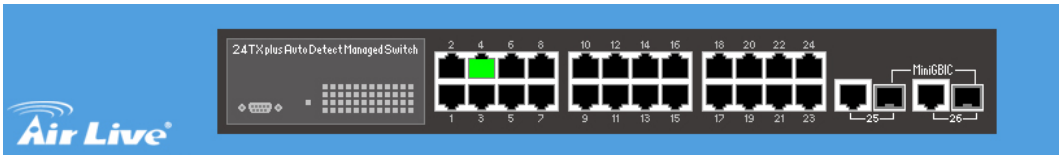
4.8 System Reboot

Reboot the Switch in software reset. Click "**Apply**" button to reboot the switch.



4.9 Panel List

Display the Switch panel GUI. When the Switch is in stacking status, it displays the slaves panel GUI. When the Switch is stand-alone status, it displays itself panel GUI. You can click the port on the panel GUI to check port current information.



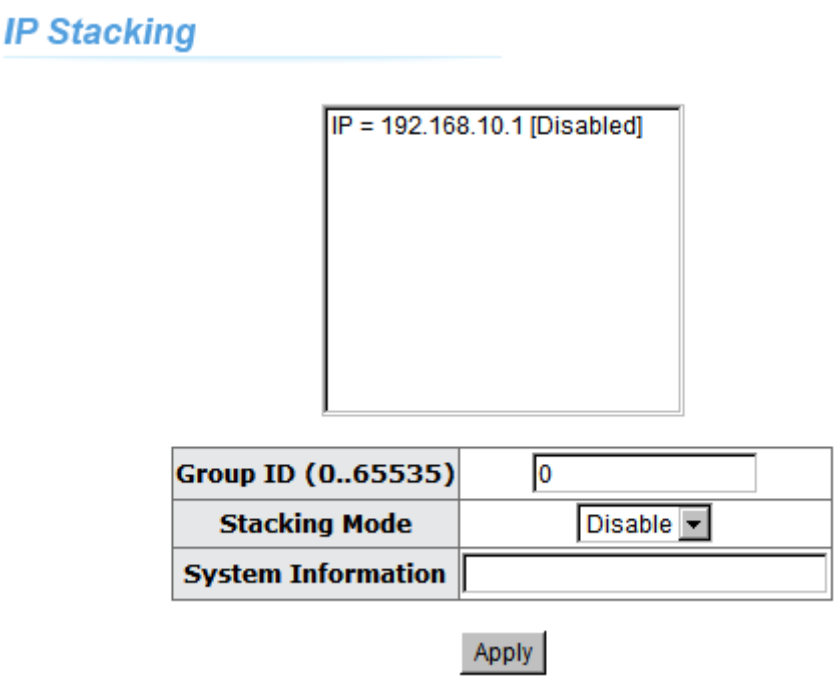
4.10 IP Stacking

This function allows Switch to stack up to 8 stackable switches as a unit group. When configuring the stacking function, beware the following points.

- Any port on the switch can be used to stack.
- Before configuring the stacking function, make sure all stack switches are in the same network.
- When configure stacking function, please must configure the master switch first.
- After stacking group has set up, all slave switches are configured through master switch. You still can directly access to slave switch, but all functions are read and view only.
- To remove the switch from stacking group, you must remove the salve switch first. When all slave switches are removed, and then you can remove the master switch from stacking group. If you remove the master switch before slave switch, go to slave switches one by one and use console configuration to re-configure the switch

configuration or you re-configure one of the slave switched as the master by console interface.

1. Click "**IP Stacking**" in the menu bar.
2. **Group ID (0...65535):** Assign a group ID for stacking group. The switches in the same stacking group have same group ID. The valid range is from 1 to 65535.
3. **Stacking Mode:** Select the stacking mode from drag down list.
   - **Disable:** It means the switch doesn't belong to any stacking group or stacking function is disabled.
   - **Master:** It means the switch is the leader (master) in the stacking group. The master switch can control all the slave switches in stacking group.
   - **Slave:** it means the switch is a slave switch of the stacking group. To configure the slave switch that you must access by the master switch.
4. **System Information**: Enter system information in box.

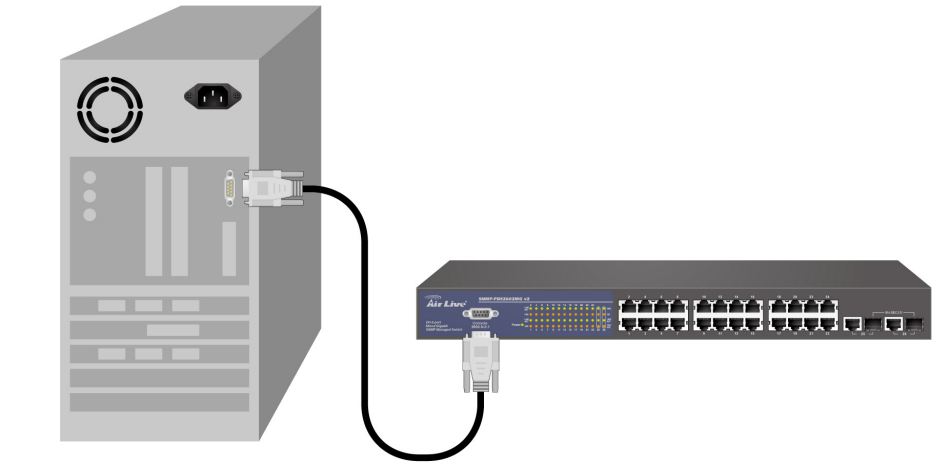


5 Console Management in SNMP-FSH2602MG v2

In this chapter, we will explain features that are available through console. For detailed descriptions on the concept and application of the settings, please refer to chapter 4.

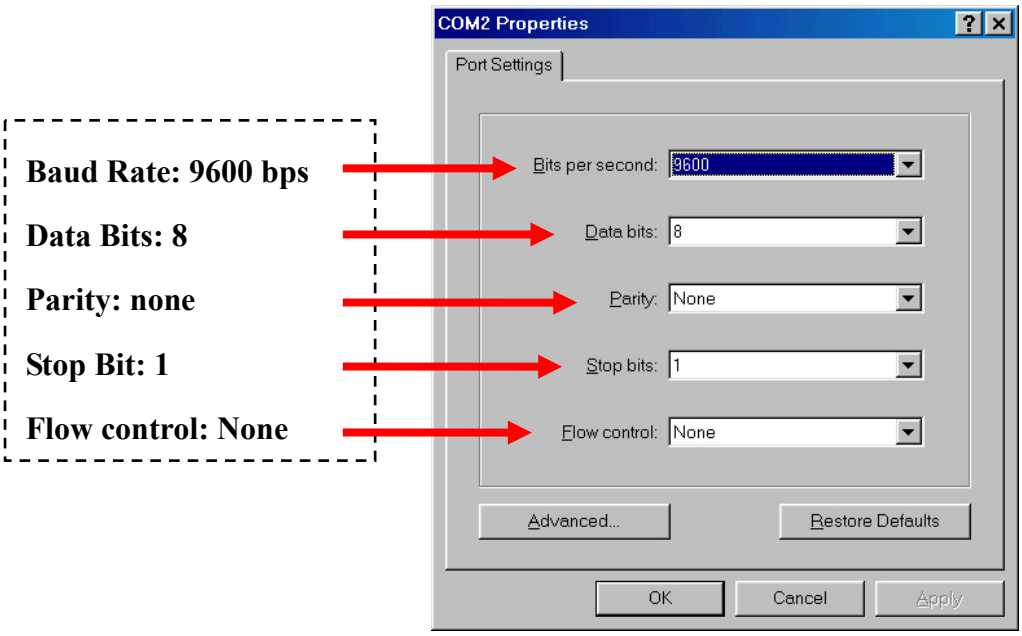
5.1 Connecting to the Console Port

The Console port is a female DB-9 connector that enables a connection to a PC or terminal for monitoring and configuring the Switch. Use the supplied RS-232 cable with a male DB-9 connector to connect a terminal or PC to the Console port.

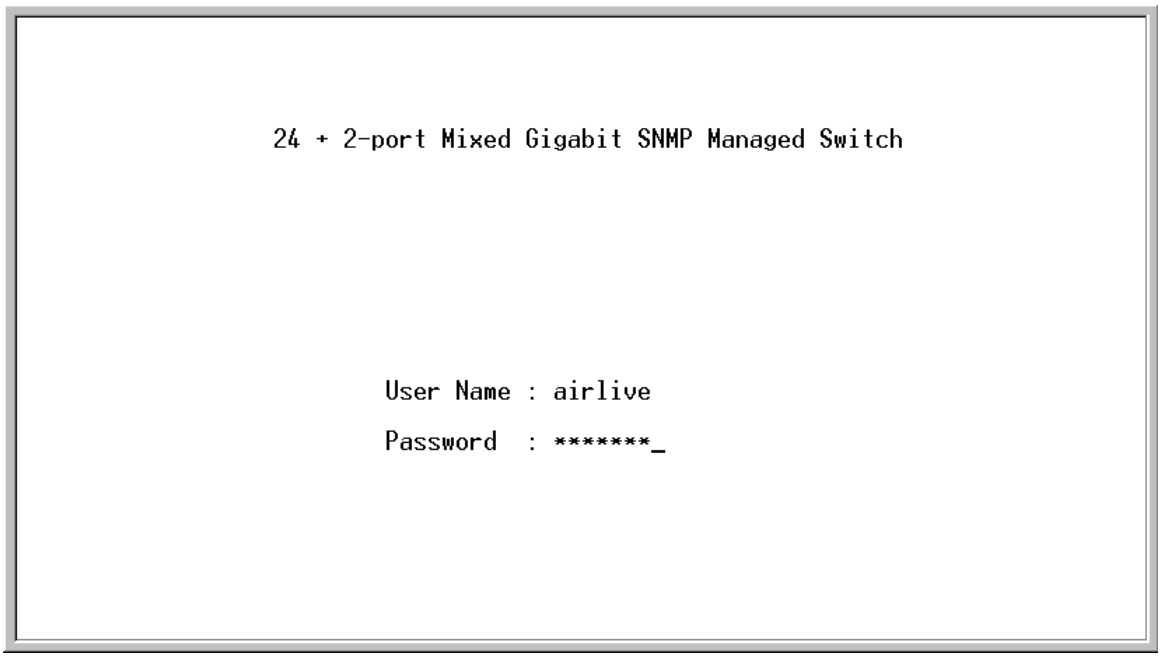


5.2 Login in the Console Interface

When the connection between Switch and PC is ready, turn on the PC and run a terminal emulation program or **Hyper Terminal** and configure its **communication parameters** to match the following default characteristics of the console port:



After finished the parameter settings, click "**OK**". When the blank screen shows up, press Enter key to bring out the login prompt. Key in the "**airlive**"(default value) for the both User name and Password (use **Enter** key to switch), then press Enter key and the Main Menu of console management appears. Please see below figure for login screen.



5.3 Main Menu

There are five selections as follow.

- **Status and Counters:** Show the status of the switch.
- **Switch Configuration:** Configure the switch.
- **Protocol Related Configuration:** Configure the protocol function.
- **System Reset Configuration:** Restart the system or reset switch to default configuration.
- **Logout:** Exit the menu line program.

- **Control Key description:**

The control keys provided in all menus:

Tab: Move the vernier to next item.

Backspace: Move the vernier to previous item.

Enter: Select item.

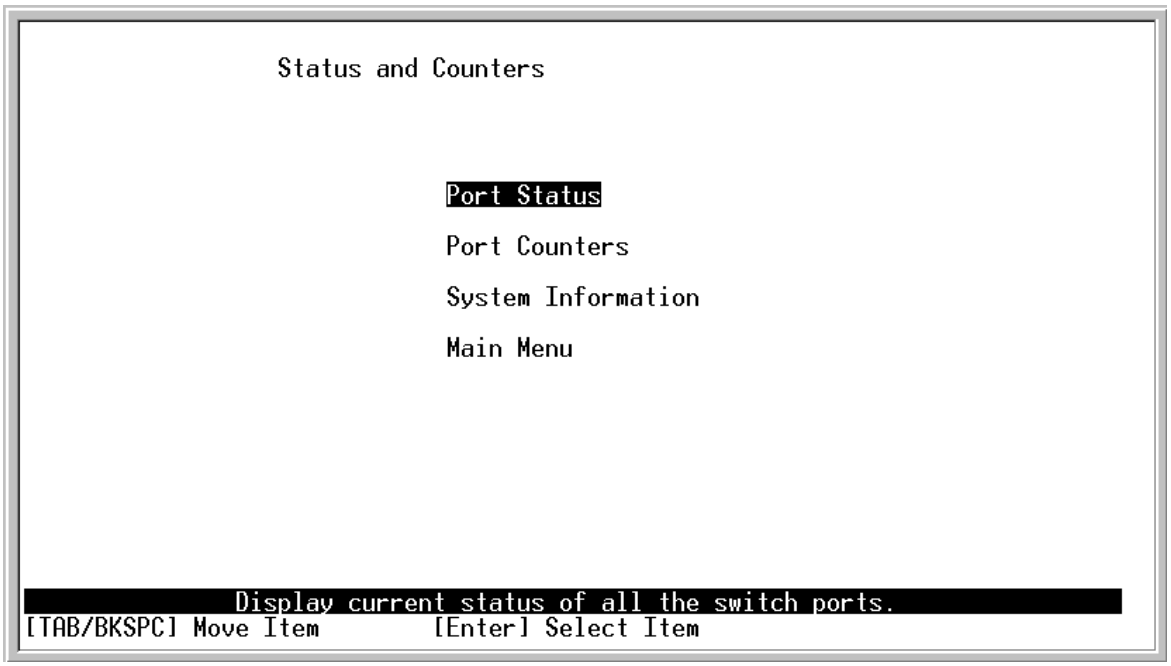
Space: Toggle selected item to next configure or change the value.

Esc: to exit the current action mode.

5.4 Function Description

5.4.1 Status and Counters

In Status and Counters, you can view Port status, counters, and configure system parameter. You can press the "**Tab**" or "**Backspace**" to choose the item, and press "**Enter**" key to select the item.

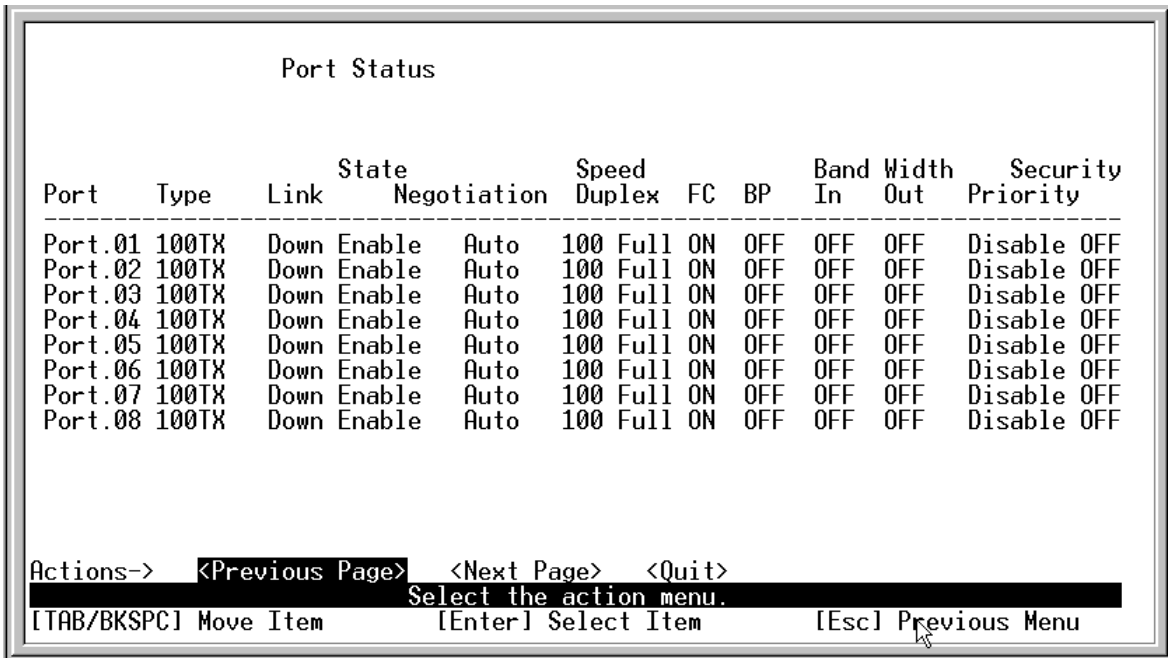


Port Status

It will display status of the port. Select the **<Previous Page>** action to display previous page. And, select the **<Next page>** action to display next page.

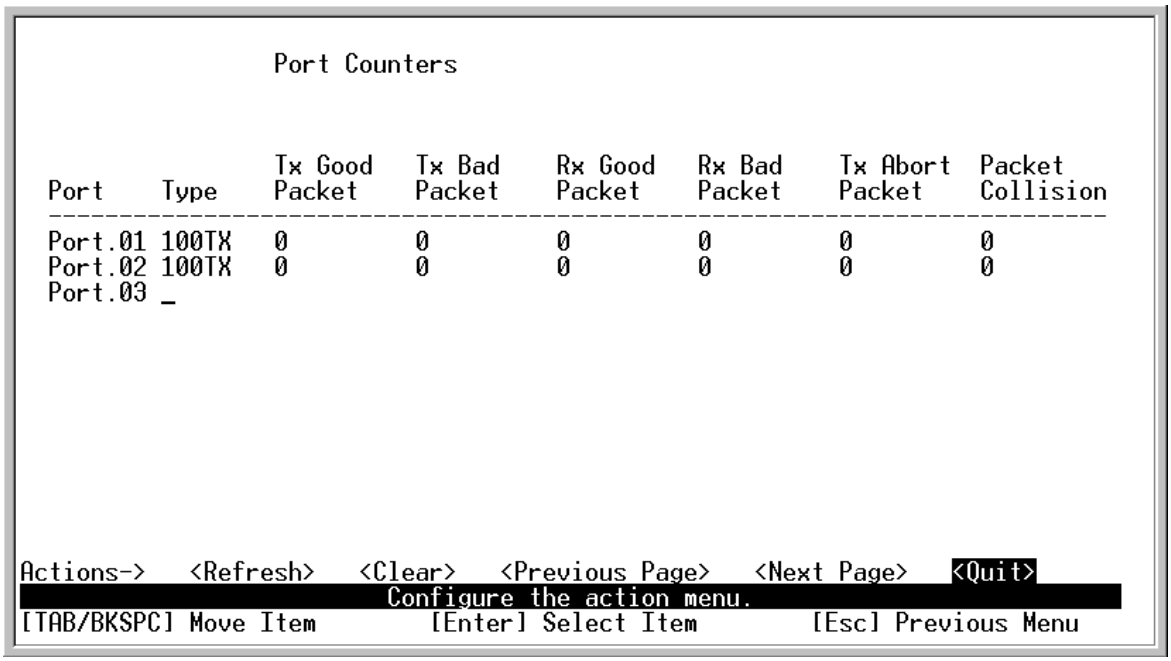
- **Type:** Display port connection speed type.
- **Link:** Display port link status. When the port is connecting with the device and work normally, the link status is "**UP**". Opposite is "**Down**".
- **State:** The port current status. "**Enable**" – it means this port working status is normal. "**Disable**" – it means this port is not function event the device is connected.
- **Negotiation:** Display the auto negotiation status.
- **Speed Duplex:** Display port speed and duplex mode.

- **FC:** Display the flow control status is “enable” or “disable”.
- **BP:** Display backpressure status.
- **Bandwidth In/Out:** Display bandwidth In/out control status.
- **Priority:** Display the port priority status.
- **Security:** Display the port security status.


Port Status
State
Speed
Band Width
Security
Port Type Link Negotiation Duplex FC BP In Out Priority
Port.01 100TX Down Enable Auto 100 Full ON OFF OFF OFF Disable OFF
Port.02 100TX Down Enable Auto 100 Full ON OFF OFF OFF Disable OFF
Port.03 100TX Down Enable Auto 100 Full ON OFF OFF OFF Disable OFF
Port.04 100TX Down Enable Auto 100 Full ON OFF OFF OFF Disable OFF
Port.05 100TX Down Enable Auto 100 Full ON OFF OFF OFF Disable OFF
Port.06 100TX Down Enable Auto 100 Full ON OFF OFF OFF Disable OFF
Port.07 100TX Down Enable Auto 100 Full ON OFF OFF OFF Disable OFF
Port.08 100TX Down Enable Auto 100 Full ON OFF OFF OFF Disable OFF
Actions-> <Previous Page> <Next Page> <Quit>
Select the action menu.
[TAB/BKSPC] Move Item [Enter] Select Item [Esc] Previous Menu

Port Counters

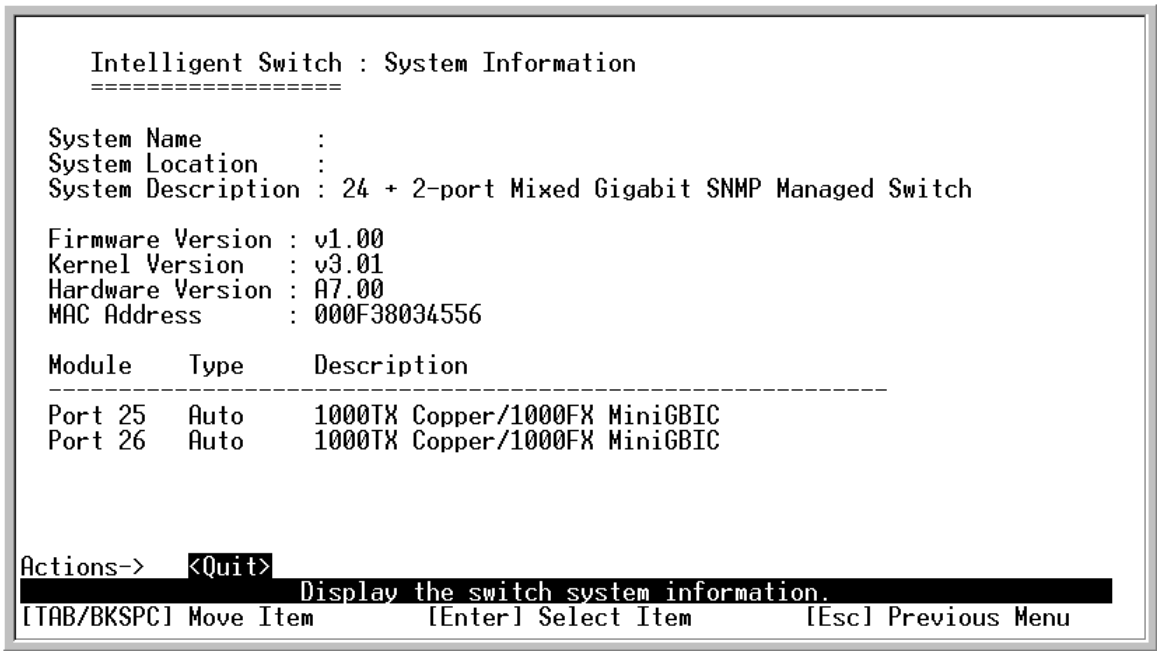
It will display the current port counter information. Select the **<Refresh>** action to get newest port counter information. Select the **<Clear>** action to set the port counter information back to 0.



System Information

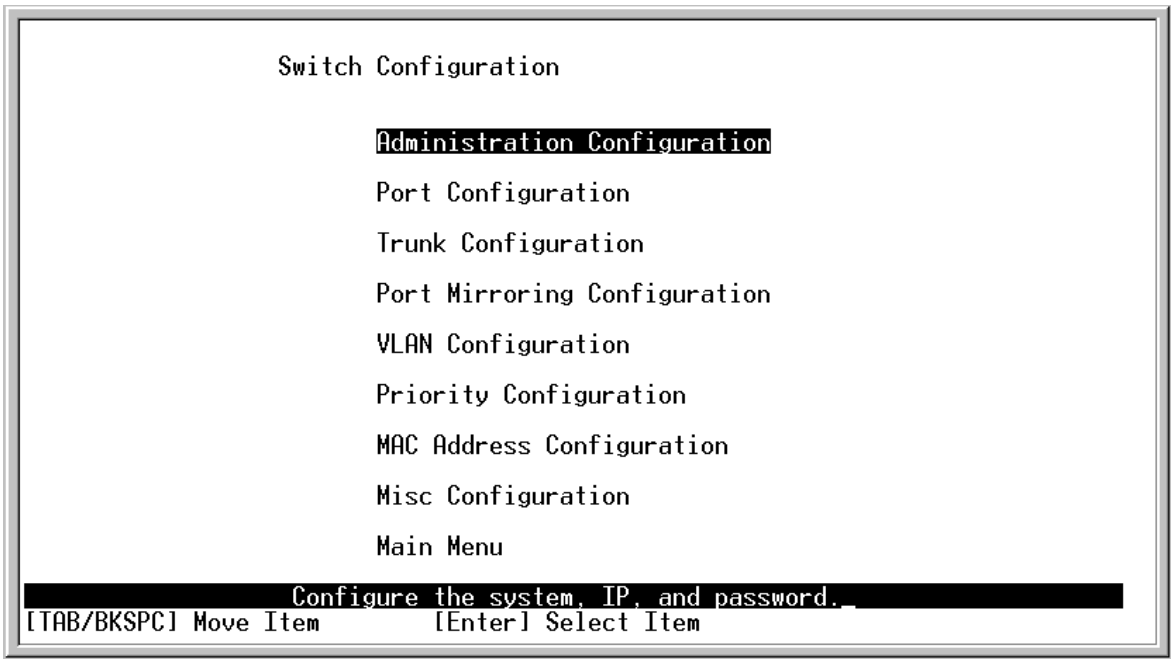
It will display the system parameter.

1. **System Name:** the name of device.
2. **System Location:** where the device is located.
3. **System Description:** the name of device type.
4. **Firmware Version:** the switch's firmware version.
5. **Hardware Version:** the switch's Hardware version.
6. **Kernel Version:** the system kernel software version.
7. **MAC Address:** The unique hardware address assigned by manufacturer.
8. **Module Information:** display the Module type that you have installed in switch.


Intelligent Switch : System Information
System Name :
System Location :
System Description : 24 + 2-port Mixed Gigabit SNMP Managed Switch
Firmware Version : v1.00
Kernel Version : v3.01
Hardware Version : A7.00
MAC Address : 000F38034556
Module Type Description
Port 25 Auto 1000TX Copper/1000FX MiniGBIC
Port 26 Auto 1000TX Copper/1000FX MiniGBIC
Actions-> <Quit>
Display the switch system information.
[TAB/BKSPC] Move Item [Enter] Select Item [Esc] Previous Menu

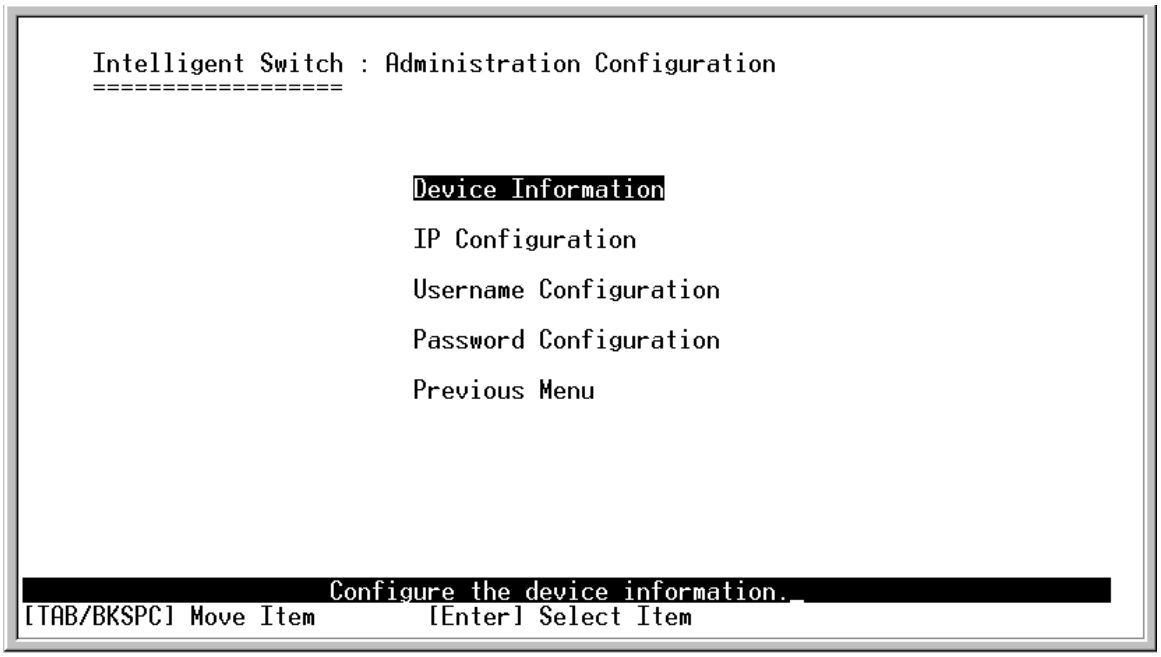
5.4.2 Switch Configuration

In Switch Configuration, it has 8 main functions – Administration, Port, Trunk, Port Mirroring, VLAN, Priority, MAC Address, and Misc Configuration. Under each function, there are more sub-functions. We will describe in following paragraph.



Administration Configuration

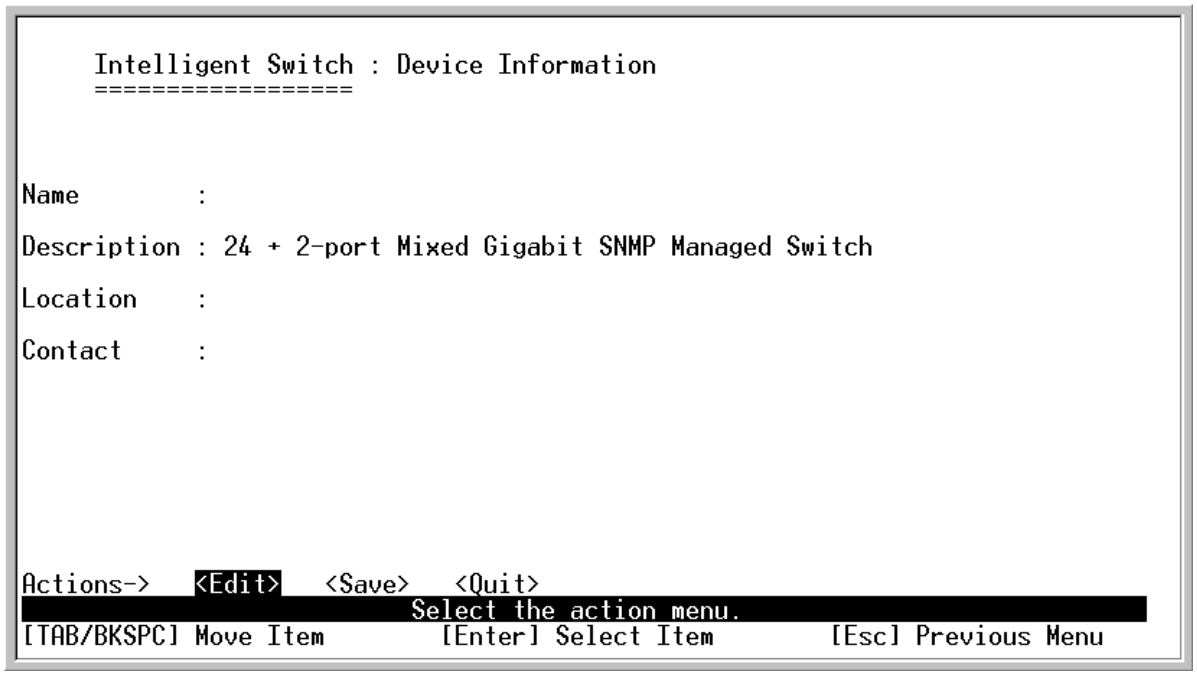
In Administration Configuration, you can configuration system parameter, IP, login username and password.



■ Device Information

You can configure the device information.

1. Select **<Edit>** action to configure.
2. **Name:** assign the name for the switch.
3. **Description:** a short description for the switch.
4. **Location:** the switch location, ex: Taipei.
5. **Contact:** the contact person or information.
6. **Select <Save>** action to save the configuration.

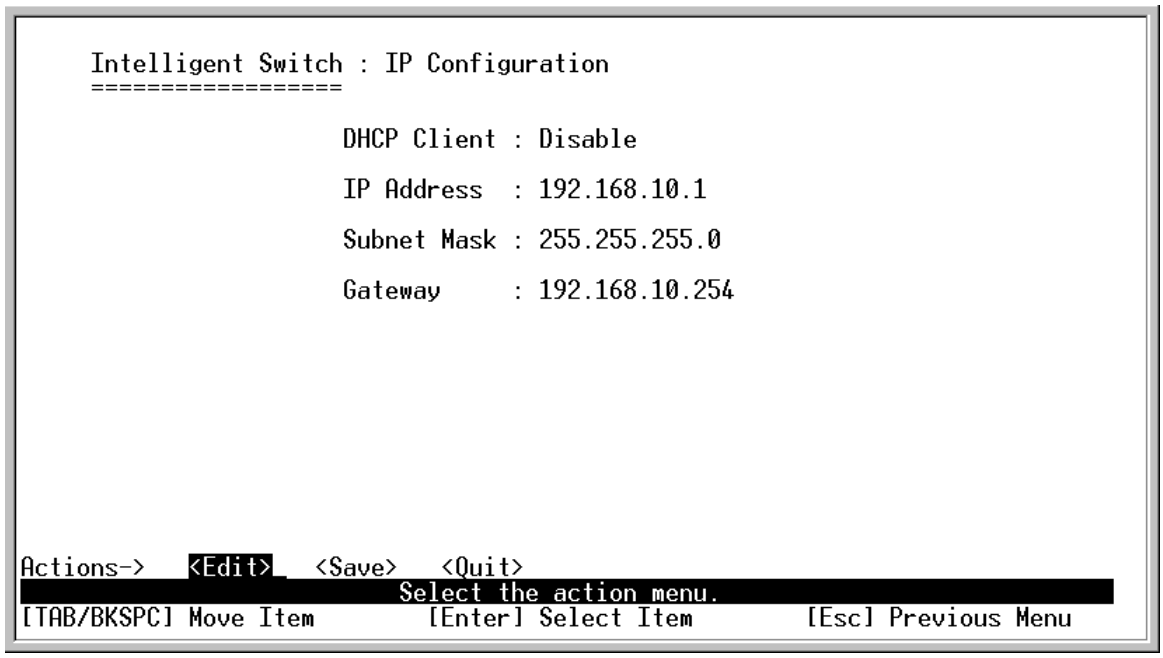

Intelligent Switch : Device Information
Name :
Description : 24 + 2-port Mixed Gigabit SNMP Managed Switch
Location :
Contact :
Actions-> <Edit> <Save> <Quit>
Select the action menu.
[TAB/BKSPC] Move Item [Enter] Select Item [Esc] Previous Menu

■ IP Configuration

You can configure the IP for this switch. The system has the default IP address. You can re-configure or use the default value.

1. Select the **<Edit>**
2. **DHCP:** Disable or enable the DHCP client function.
3. **IP Address:** Assign the switch IP address. The default IP is 192.168.16.1.
4. **Subnet Mask:** Assign the switch IP subnet mask.
5. **Gateway:** Assign the switch gateway. The default value is 192.168.16.254.
6. Select **<Save>** action to save the configuration.

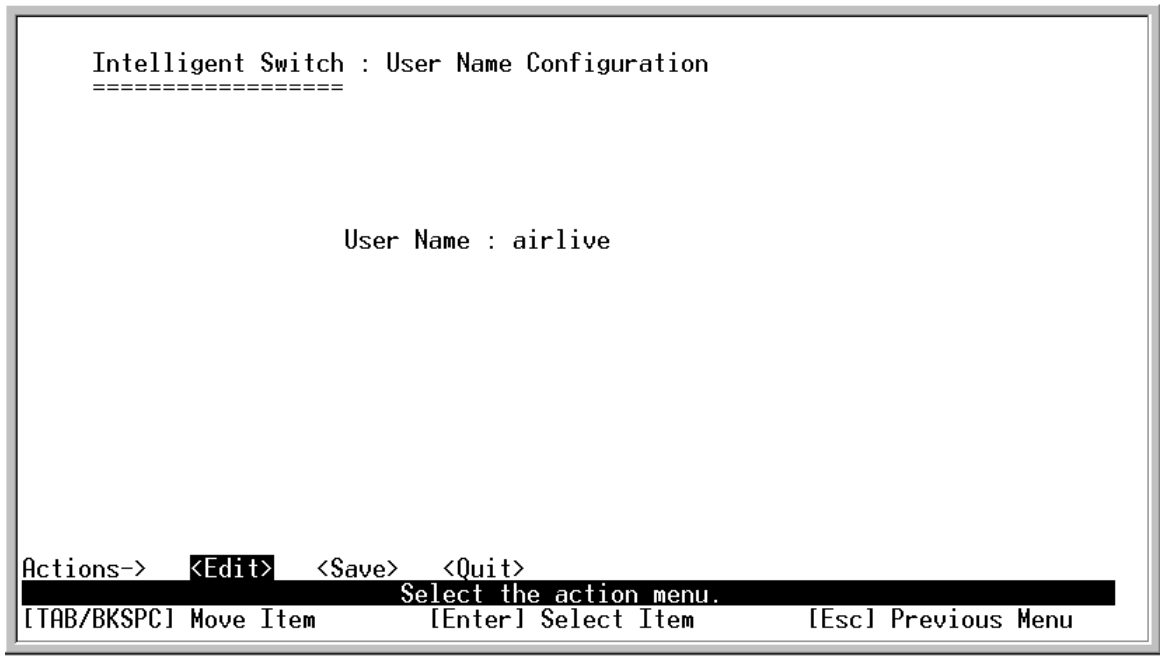
[Note] Always restart the switch after finished the setup.


Intelligent Switch : IP Configuration
DHCP Client : Disable
IP Address : 192.168.10.1
Subnet Mask : 255.255.255.0
Gateway : 192.168.10.254
Actions-> <Edit> <Save> <Quit>
Select the action menu.
[TAB/BKSPC] Move Item [Enter] Select Item [Esc] Previous Menu

■ Username Configuration

You can change the console and web management login user name.

1. Select the **<Edit>**
2. Enter the new user name
3. Select the **<Save>**


Intelligent Switch : User Name Configuration
User Name : airlive
Actions-> <Edit> <Save> <Quit>
Select the action menu.
[TAB/BKSPC] Move Item [Enter] Select Item [Esc] Previous Menu

■ Password Configuration

You can change the console and web management login password.

1. Select the **<Edit>**
2. **Old Password:** enter the old password.
3. **New Password:** enter the new password.
4. **Enter Again:** reenter the new password for confirmation.
5. Select the **<Save>**

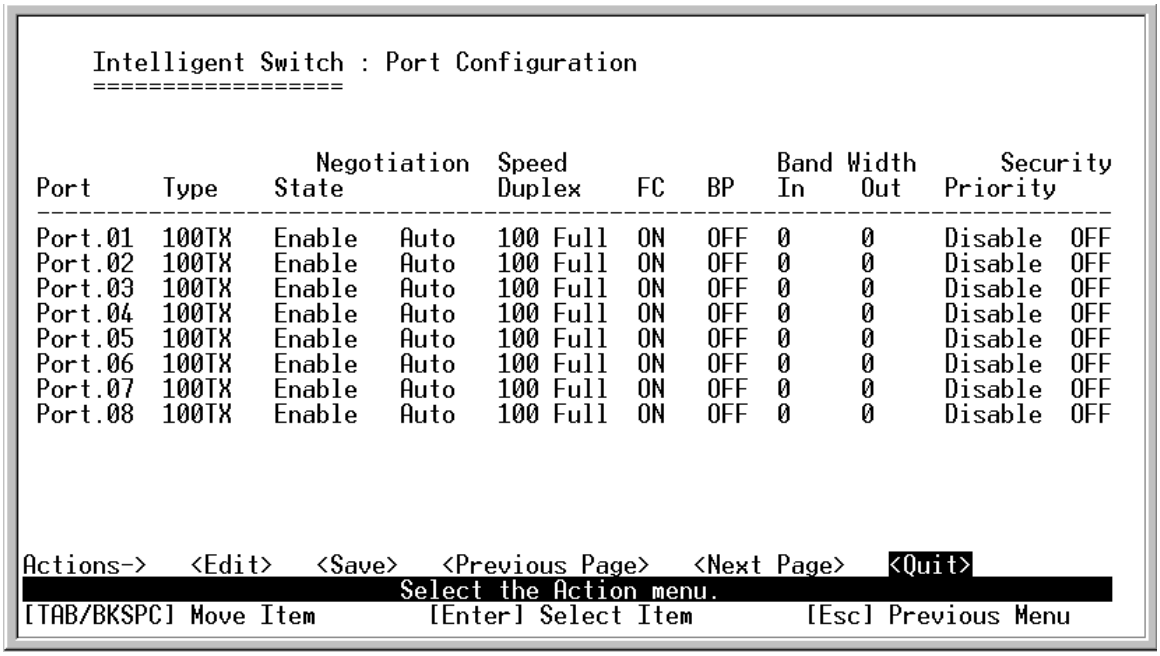
Intelligent Switch : Password Configuration
Old Password :
New Password :
Enter Again :
Actions-> <Edit> <Save> <Quit>
Select the action menu.
[TAB/BKSPC] Move Item [Enter] Select Item [Esc] Previous Menu

Port Configuration

You can set up every port status.

1. Select **<Edit>**
2. Use "**Tab**" key to move between items.
3. **State:** Current port status. The port can be set to disable or enable mode. If the port setting is disable then will not receive or transmit any packet.
4. **Negotiation:** set auto negotiation status of port.
5. **Speed/Duplex:** set the port link speed and duplex mode.

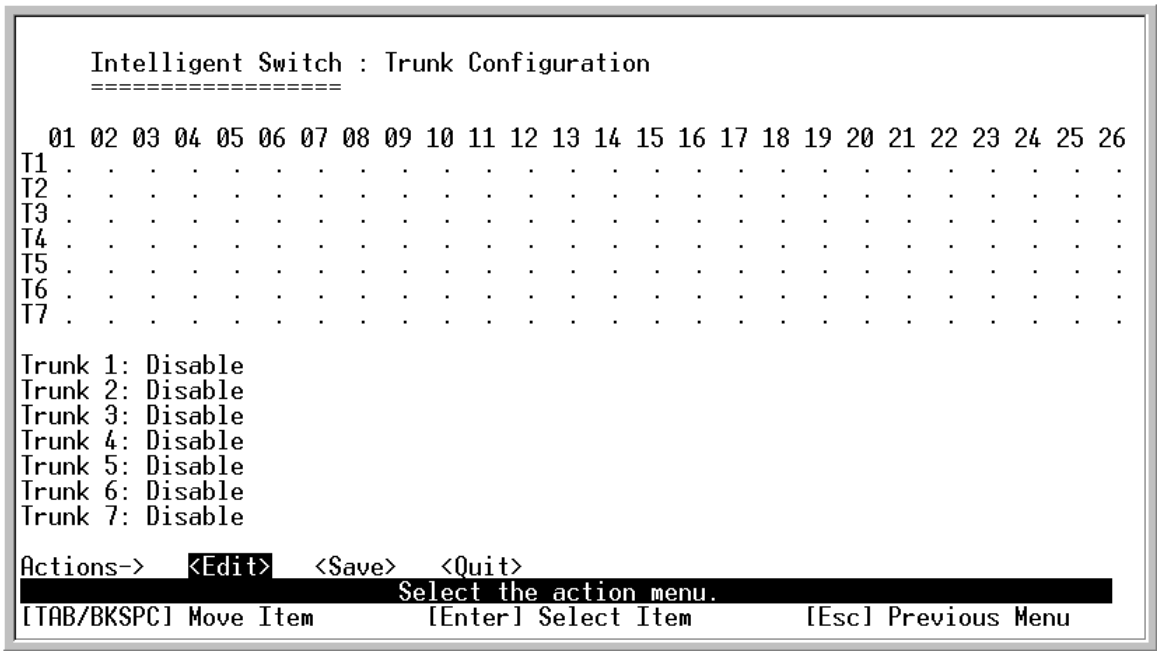
6. **FC:** enable or disable **Flow control** function (Flow control for full duplex link mode).
7. **BP:** enable or disable **Back Pressure** function (Backpressure for half duplex mode).
8. **Bandwidth In/Out:** per port packet transmission rate control. Per level is 100Kbps. It supports individual control method of TX and RX.
9. **Priority:** set port to high or low priority.
10. **Security:** enable or disable port security function.
11. Select the **<Save>**.


Intelligent Switch : Port Configuration
Port Type Negotiation State Speed Duplex FC BP Band Width In Band Width Out Security Priority
Port.01 100TX Enable Auto 100 Full ON OFF 0 0 Disable OFF
Port.02 100TX Enable Auto 100 Full ON OFF 0 0 Disable OFF
Port.03 100TX Enable Auto 100 Full ON OFF 0 0 Disable OFF
Port.04 100TX Enable Auto 100 Full ON OFF 0 0 Disable OFF
Port.05 100TX Enable Auto 100 Full ON OFF 0 0 Disable OFF
Port.06 100TX Enable Auto 100 Full ON OFF 0 0 Disable OFF
Port.07 100TX Enable Auto 100 Full ON OFF 0 0 Disable OFF
Port.08 100TX Enable Auto 100 Full ON OFF 0 0 Disable OFF
Actions-> <Edit> <Save> <Previous Page> <Next Page> <Quit>
Select the Action menu.
[TAB/BKSPC] Move Item [Enter] Select Item [Esc] Previous Menu

Trunk Configuration

You can configure port trunk group.

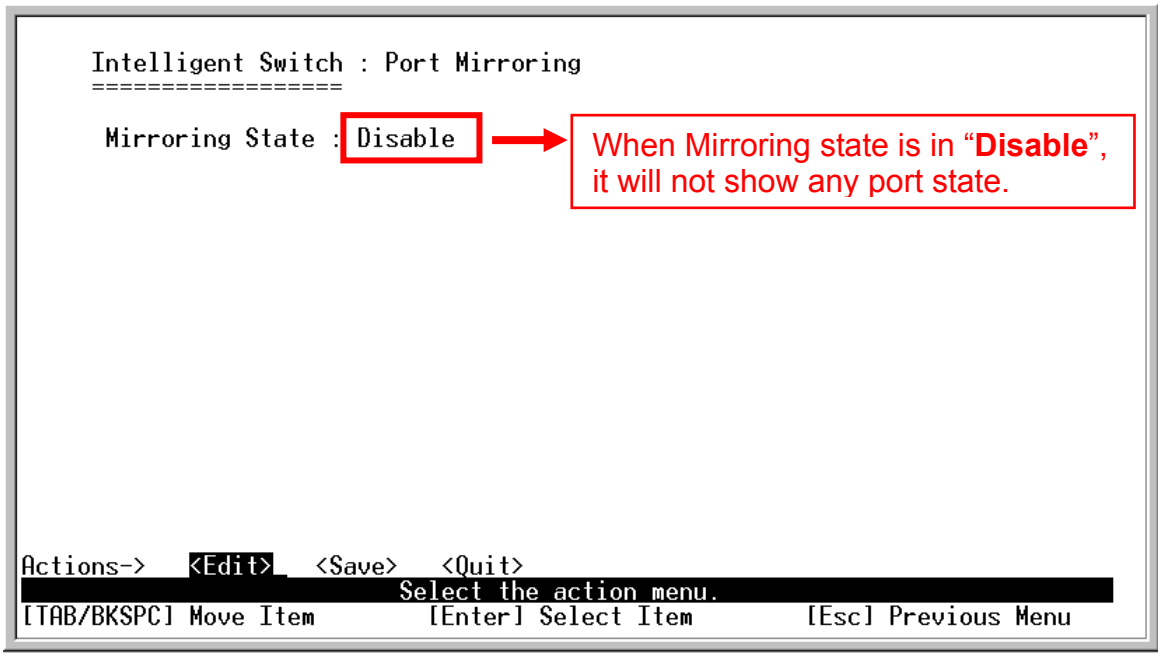
1. Select **<Edit>**
2. Using "**Tab**" key move to the port that want to be added into trunk group.
3. Using "**Space**" key to mark the port as "∗".
4. Using **Tab** key move to "**Trunk #**" (ex. Trunk 1, Trunk 2…) to change the Trunk # value to "**Static**".
5. Save the configuration by selecting **<Save>**.



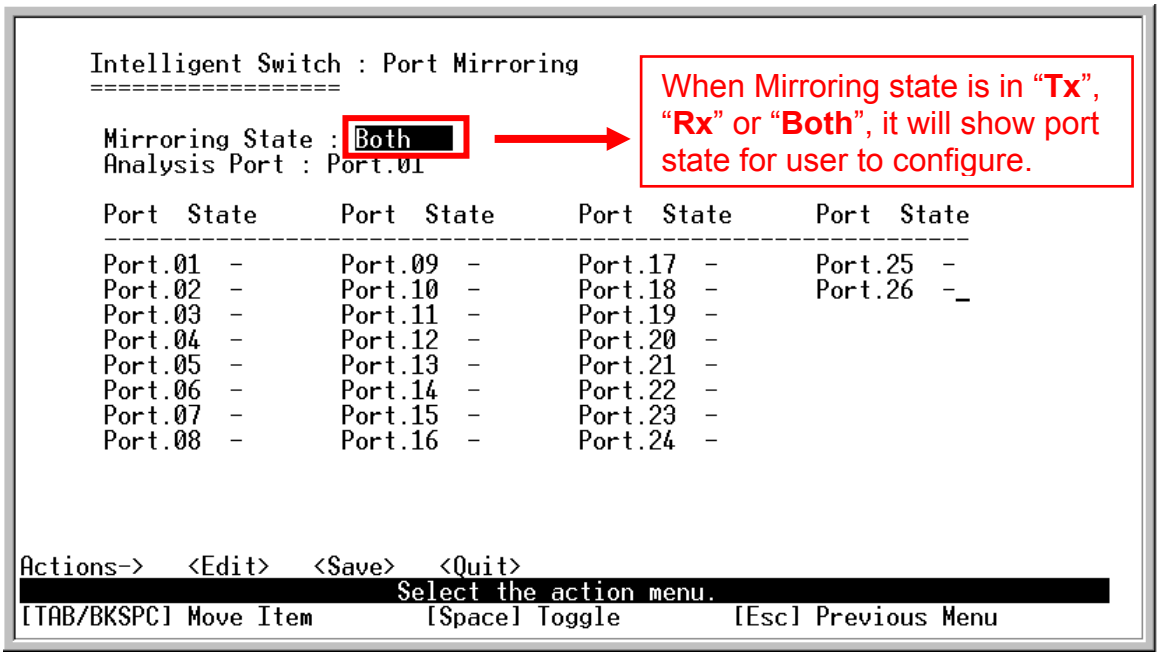
Port Mirroring

The port mirroring is a method for monitor traffic of switched networks. The specific port can monitor traffic through the mirror ports. The monitored ports in or out traffic will be duplicated into monitoring port.

1. Select the **<Edit>**
2. **Mirroring State:** Select the port-mirroring mode. The default value is "**Disable**". To start port mirroring, you must select one of port mirroring mode.
   - **RX:** RX packet only
   - **TX:** TX packet only
   - **Both:** RX and TX packet

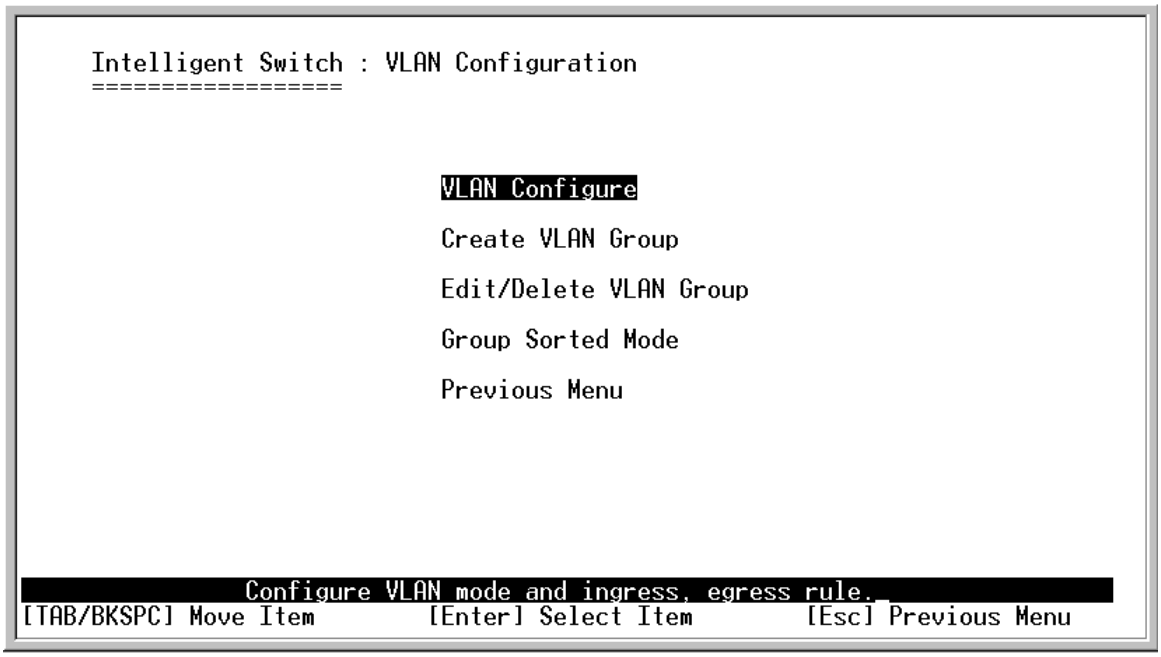

Intelligent Switch : Port Mirroring
Mirroring State : Disable
When Mirroring state is in "Disable", it will not show any port state.
Actions-> <Edit> <Save> <Quit>
Select the action menu.
[TAB/BKSPC] Move Item [Enter] Select Item [Esc] Previous Menu

3. **Analysis port:** Set the destination port of mirroring packet. All of the packets of mirroring port will be duplicated and sent to Analysis port.
4. Use "**Space**" key to mark the mirroring port.
5. Select the **<Save>.**


Intelligent Switch : Port Mirroring
Mirroring State : Both
Analysis Port : Port.01
When Mirroring state is in "Tx", "Rx" or "Both", it will show port state for user to configure.
Port State Port State Port State Port State
Port.01 - Port.09 - Port.17 - Port.25 -
Port.02 - Port.10 - Port.18 - Port.26 -
Port.03 - Port.11 - Port.19 -
Port.04 - Port.12 - Port.20 -
Port.05 - Port.13 - Port.21 -
Port.06 - Port.14 - Port.22 -
Port.07 - Port.15 - Port.23 -
Port.08 - Port.16 - Port.24 -
Actions-> <Edit> <Save> <Quit>
Select the action menu.
[TAB/BKSPC] Move Item [Space] Toggle [Esc] Previous Menu

VLAN Configuration

You can configure VLAN in VLAN Configuration. There are four functions in VLAN Configuration mode: VLAN Configuration, Create a VLAN Group, Edit/Delete VLAN Group and Group Sorted Mode. Follow the below description to configure VLAN.



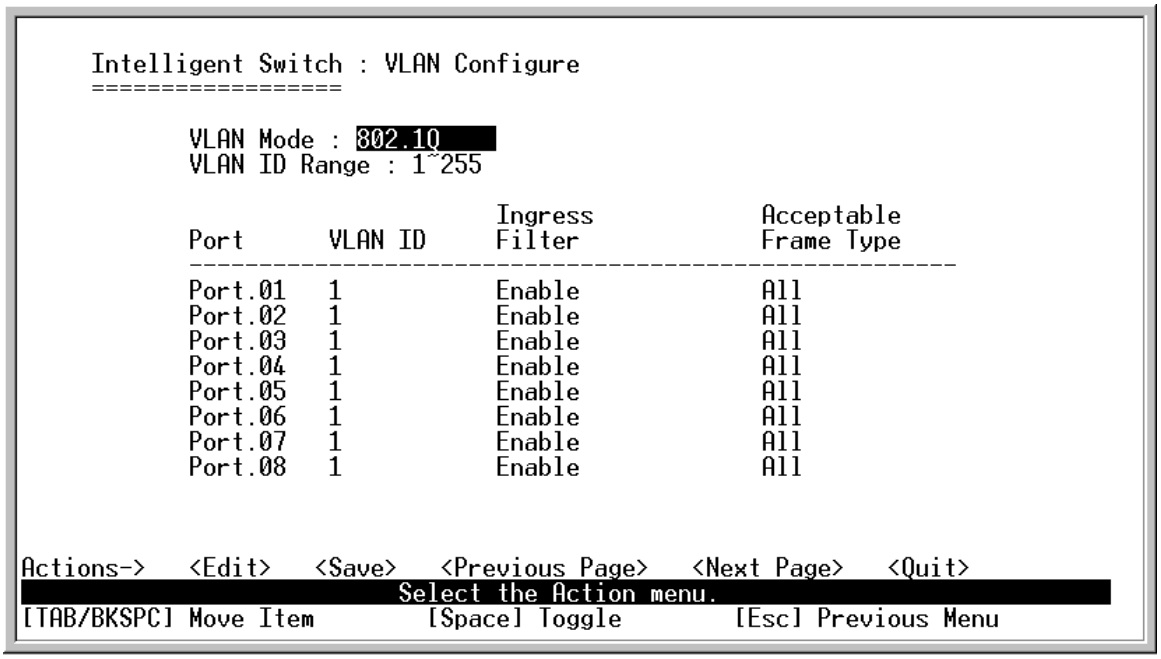
■ VLAN Configure

Before starting to configure VLAN, you must select the VLAN mode in VLAN Configure function. Otherwise, user cannot create any new VLAN.

1. Select the **<Edit>**.
2. Select the VLAN mode by using "**Space**" key. There are two VLAN modes: Port Based mode and 802.1Q mode.
   - **802.1Q VLAN mode:** configuration VLAN ID, Ingress Filter, and Acceptable Frame Type.
     - **VLAN ID (Port VID: 1~255):** Type the PVID.
     - **Ingress Filter:** It matches that Ingress Filtering Rule 1 on web. Only forward packets with VID matching this port's configured VID. Press "**Space**" key to choose forward or drop the frame that VID not matching this port's configured VID.
     - **Acceptable Frame type:** It matches that Ingress Filtering Rule 2 on web. Drop untagged frame. Press "**Space**" key to select drop or forward the untagged

frame.

Select **<Save>** to save the configuration.

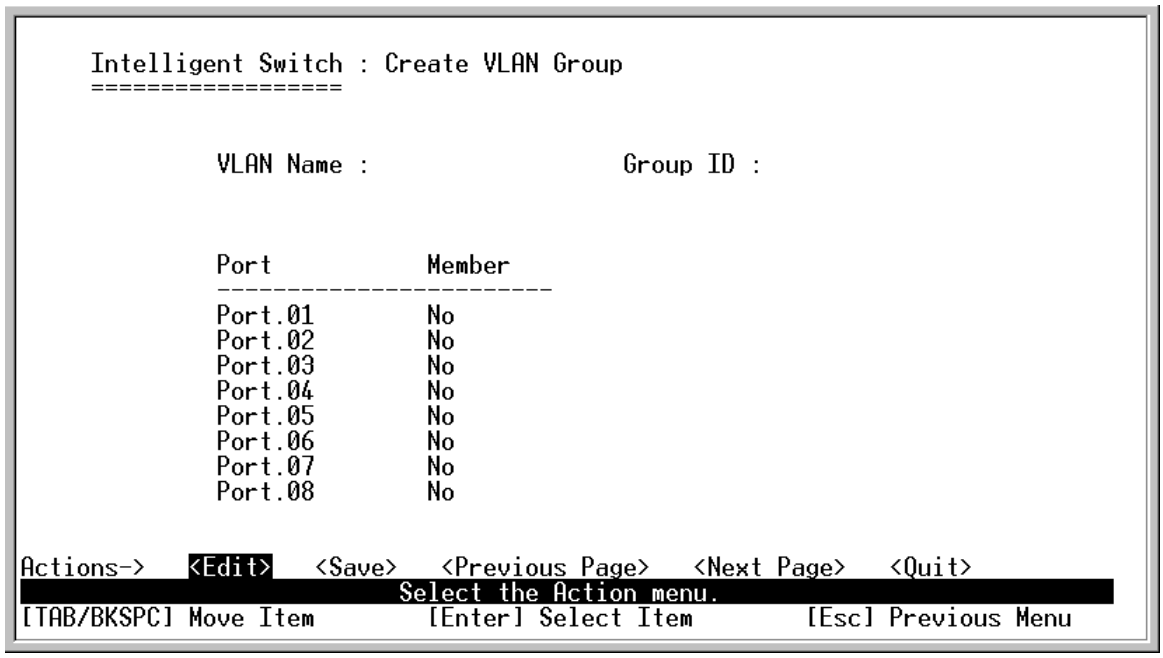


- **Create VLAN Group**

Create Port-Based VLAN

1. Select **<Edit>.**
2. **VLAN Name:** Type a name for the new VLAN, ex: VLAN01.
3. **Group ID:** Type the VLAN group ID. The group ID rang is from 1 to 4094.
4. **Member:** Press ”**Space**” key to change the member value. There are two types to selected:
   a. **Member:** the port is a member port.
   b. **NO:** it means that the port is NOT a member port.
5. Press **“ESC”** key to go back action menu line.
6. Select **<Save>** to save the configuration.

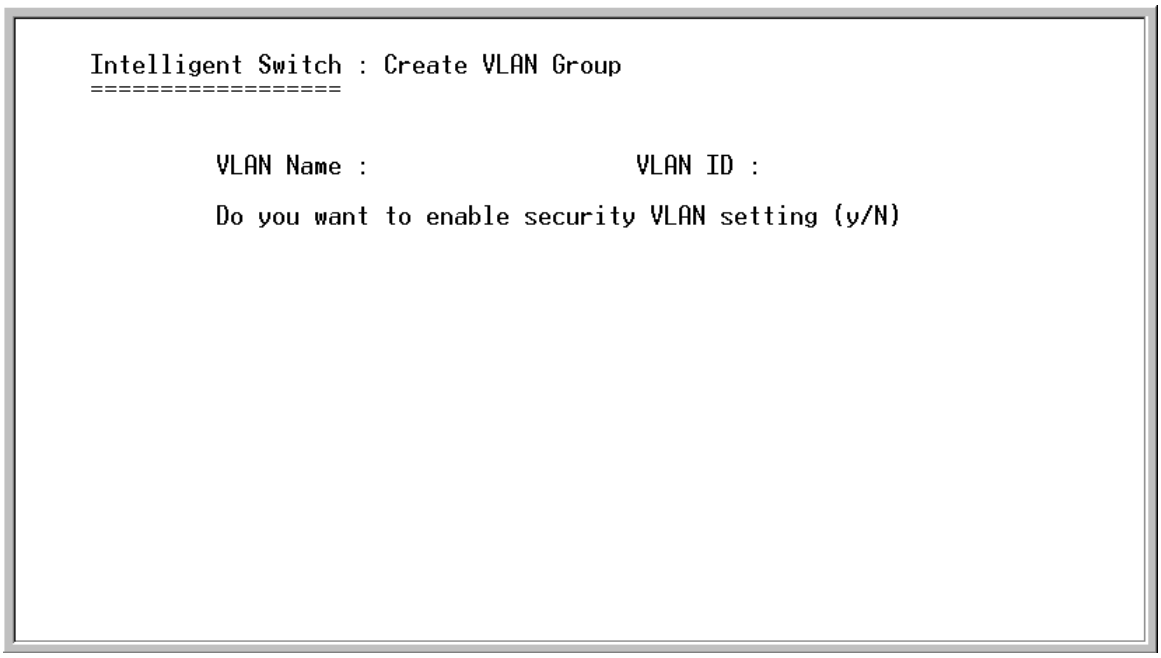
NOTE: If you had configured the trunk groups, you can see it (ex: Trunk 1, Trunk 2…) in the port list. You also can configure the trunk group as the VLAN member.



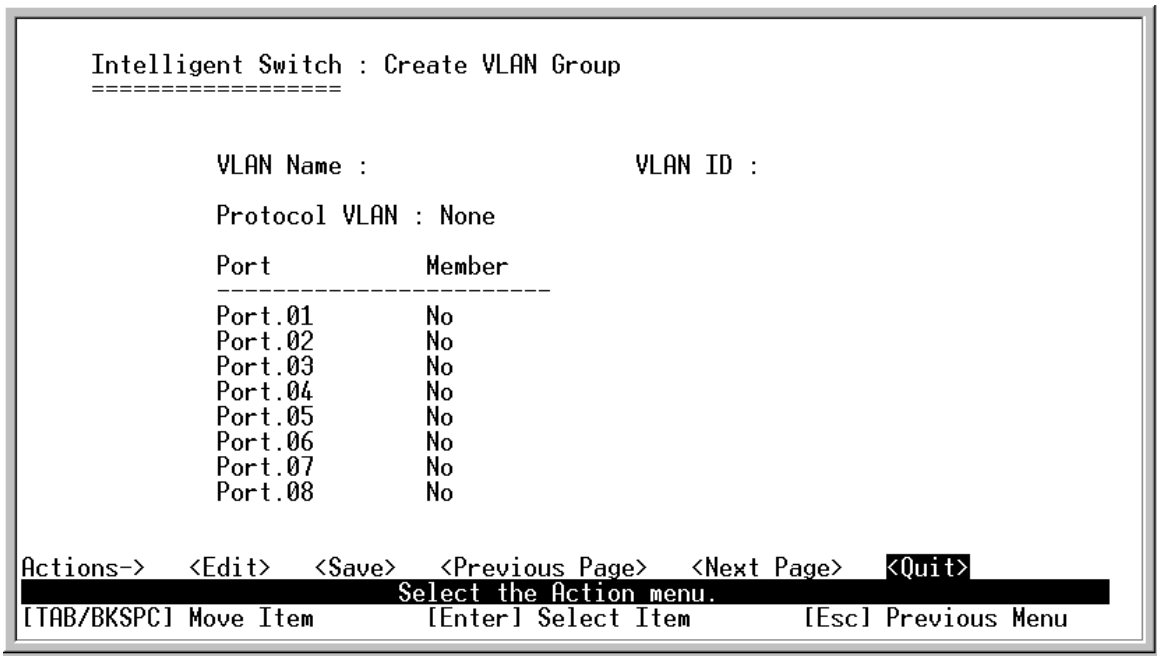
- **Create 802.1Q VLAN**

1. **Enable security VLAN setting:** Select to enable or disable security VLAN group. When you select to enable security VLAN group, only the members in this VLAN group can access to the switch. The steps of setting security VLAN refer to the following step 2~ 8. After you have configured the security VLAN group, you can continue to create other VLAN groups. When you don't select to configure security VLAN group, then just create VLAN group refer to following step 2 ~ 8.

   Note: There is only one security VLAN group.



2. Select **<Edit>**.
3. **VLAN Name:** Type a name for the new VLAN, ex: VLAN01.
4. **VLAN ID:** Type a VID (between 1~4094). The default is 1. There are 256 VLAN groups to provided configure.
5. **Protocol VLAN:** Press "**Space**" key to choose protocols type.
6. **Member:** Press "**Space**" key to change the member value.
   - **Untagged:** this port is the member port of this VLAN group and outgoing frames are NO VLAN-Tagged frames.
   - **Tagged:** this port is the member port of this VLAN group and outgoing frames are VLAN-Tagged frames.
   - **NO:** it means that the port is NOT member of this VLAN group.
7. Press "**ESC**" key to go back action menu line.
8. Select **<Save>** to save the configuration.



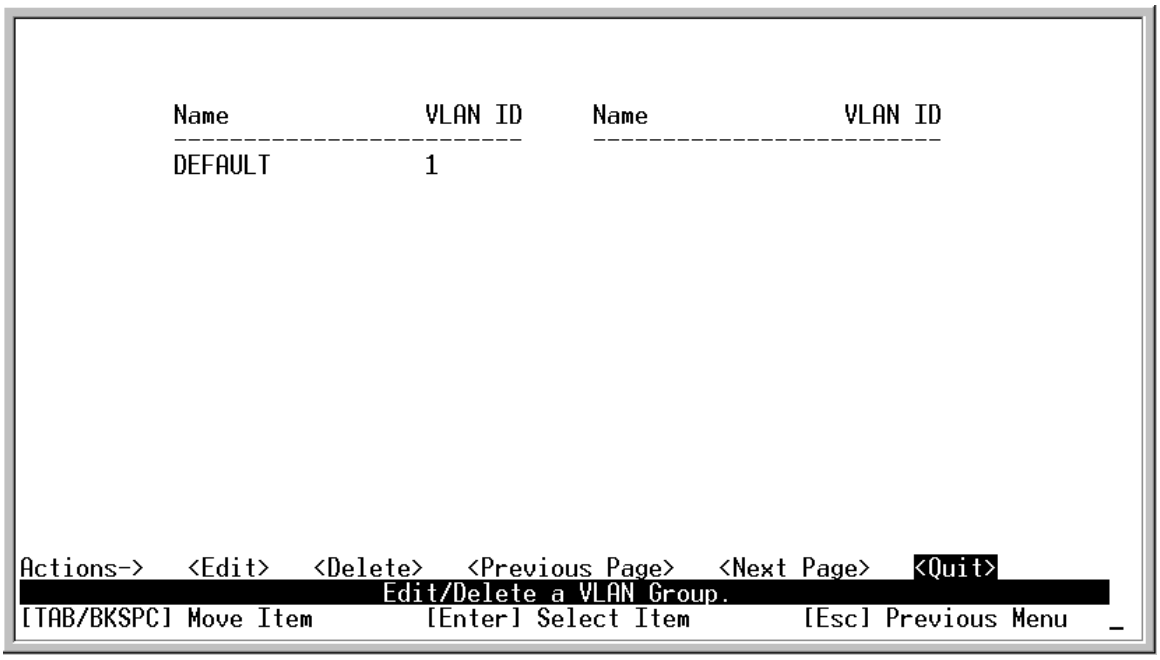
- **Edit/Delete VLAN Group**

User can edit or delete a VLAN group.

1. Select **<Edit>** or **<Delete>** action.
2. Select the VLAN group that you want to edit or delete, then press enter.
3. In **<Edit>** action, user can modify the member port and remove member ports from this VLAN group.
4. After edit or delete the VLAN, select **<Save>** action to save all configures value.

NOTE:

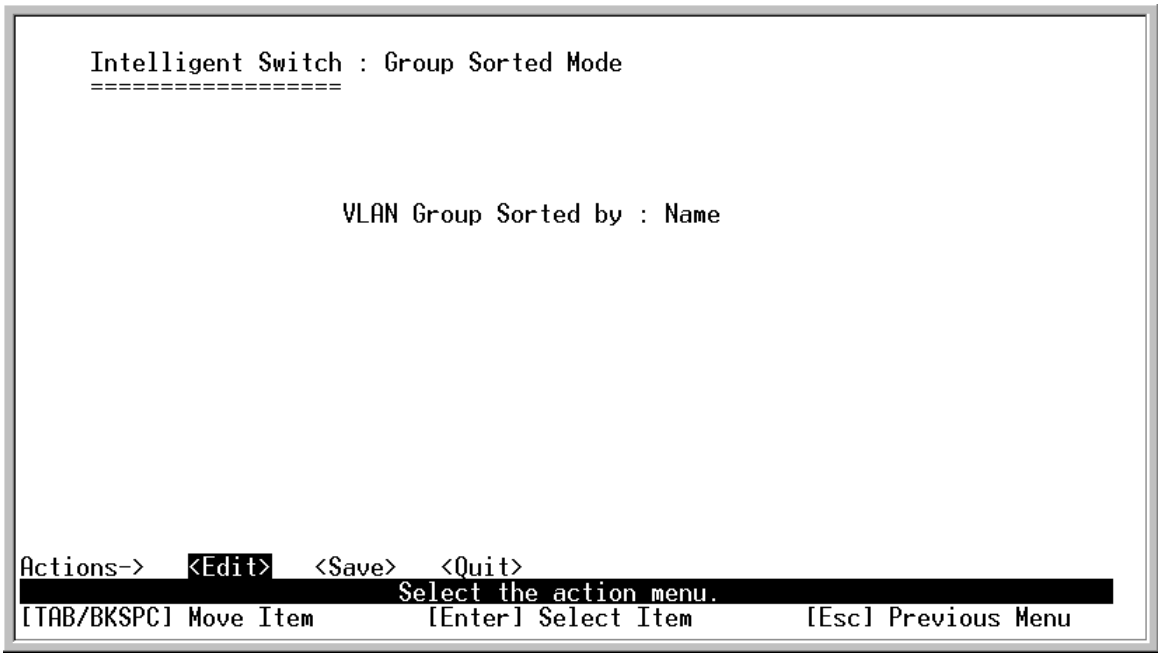
1. The VLAN Name and VLAN ID cannot modify.
2. In 802.1Q VLAN mode, the default VLAN can't be deleted.
3. In Port Base VLAN mode, there is no default VLAN.



- **Group Sorted Mode**

You can select VLAN groups sorted mode: **Name** or **VLAN ID**. In the Edit/Delete a VLAN group page will display the result.

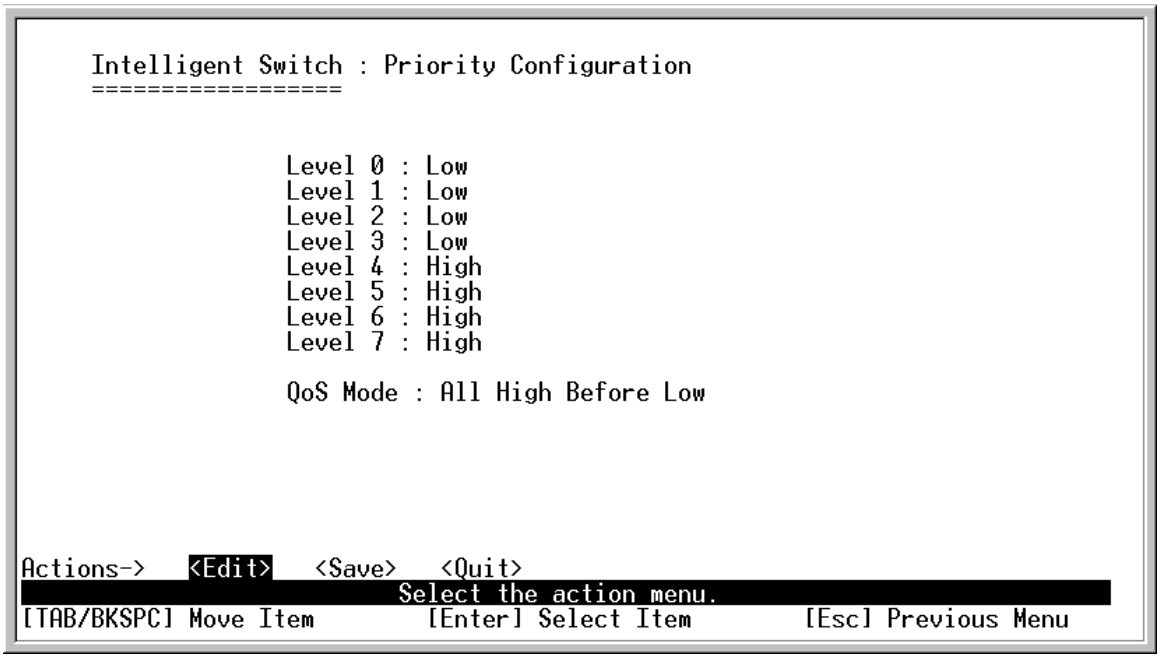
1. Select **<Edit>**
2. Use "**Space**" key to select the sort mode.
3. Select **<Save>**



Priority Configuration

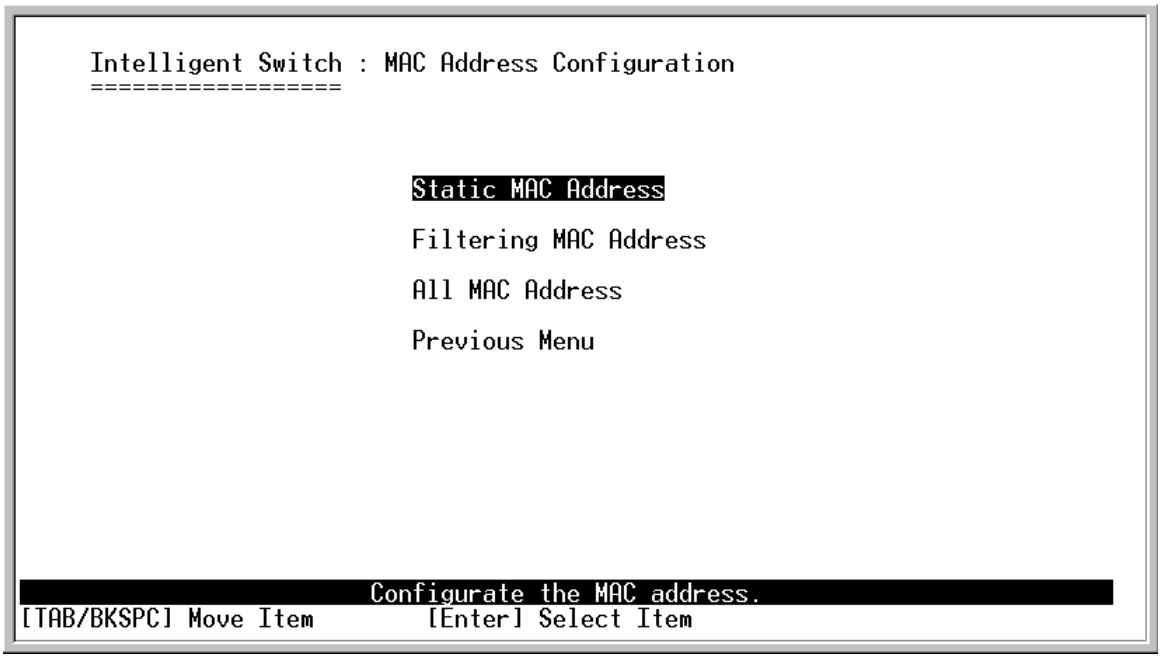
You can configure port priority level. There are 0~7-priority level can map to high or low queue.

1. Select **<Edit>**.
2. Set the Level 0~7 priority, use "**Space**" key to change the value.
3. Press "**Space**" key to select the priority level mapping to high or low queue.
4. **Qos Mode:** select the mode to process incoming packets.
   - **First Come first service:** the switch will process the packet that is coming first.
   - **All High Before low:** the packet priority is high will be process before the packet priority is low.
   - **Weight Round Ration 2:1:** the switch will process 2 high priority packets first, the process 1 low priority packet.
   - **Weight Round Ration 3:1:** the switch will process 3 high priority packets first, the process 1 low priority packet.
   - **Weight Round Ration 4:1:** the switch will process 4 high priority packets first, the process 1 low priority packet.
   - **Weight Round Ration 5:1:** the switch will process 5 high priority packets first, the process 1 low priority packet.
   - **Weight Round Ration 6:1:** the switch will process 6 high priority packets first, the process 1 low priority packet.
   - **Weight Round Ration 7:1:** the switch will process 7 high priority packets first, the process 1 low priority packet.
5. Press "**ESC**" goes back action menu line.
6. Select **<Save>** to save all configure value.


Intelligent Switch : Priority Configuration
Level 0 : Low
Level 1 : Low
Level 2 : Low
Level 3 : Low
Level 4 : High
Level 5 : High
Level 6 : High
Level 7 : High
QoS Mode : All High Before Low
Actions-> <Edit> <Save> <Quit>
Select the action menu.
[TAB/BKSPC] Move Item [Enter] Select Item [Esc] Previous Menu

MAC Address Configuration

In MAC Address Configuration, you can configure Static MAC Address, Filtering MAC Address, and All MAC Address.



■ Static MAC Address

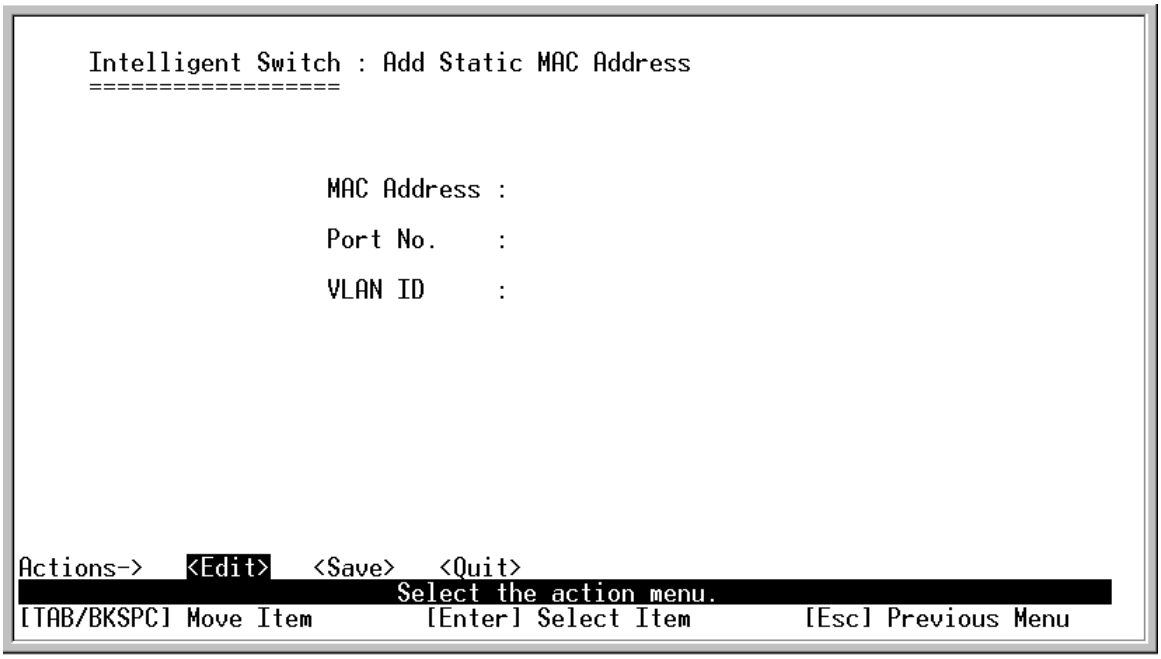
When you add a static MAC address, it remains in the switch's address table, regardless of whether the device is physically connected to the switch. This saves the switch from having to re-learn a device's MAC address when the disconnected or powered-off device is active on the network again. You can add / modify / delete a static MAC address.

Add the Static MAC Address

You can add static MAC address in switch MAC table.

1. Select **<Add>** → **<Edit>** key to add the static MAC address.
2. **MAC Address:** Enter the MAC address of the port that should permanently forward traffic, regardless of the device network activity.
3. **Port No.:** Press "**Space**" key to select the port number.
4. **VLAN ID:** Enter the Mac address's VLAN ID, if the Mac address belongs to any VLAN group.

   Note: if user does not do any VLAN configuration in advance, the setting of VALN ID will not showed in the screen.
5. Press "**ESC**" to go back action menu line.
6. Select **<Save>** to save all configure value.


Intelligent Switch : Add Static MAC Address
MAC Address :
Port No. :
VLAN ID :
Actions-> <Edit> <Save> <Quit>
Select the action menu.
[TAB/BKSPC] Move Item [Enter] Select Item [Esc] Previous Menu

Edit static MAC address

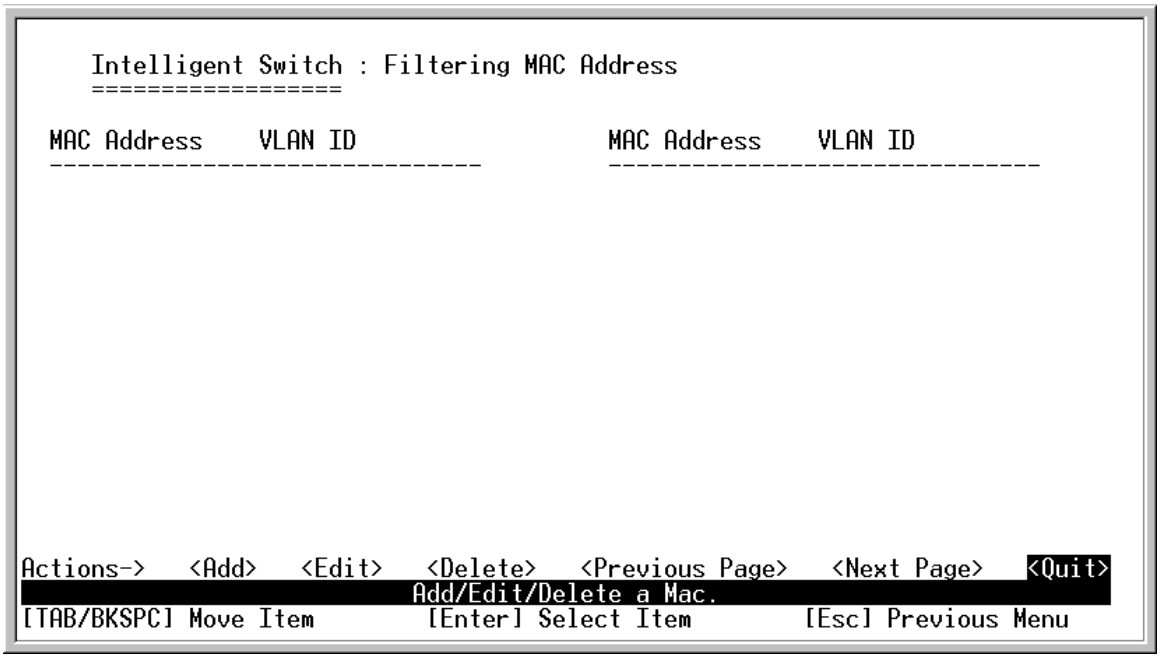
1. Select **<Edit>**.
2. Choose the MAC address that you want to modify and then press "**Enter**".
3. Press **<Edit>** key to modify.
4. Press "**ESC**" to go back action menu line.
5. Select **<Save>** to save all configure value.

Delete static MAC address

1. Select **<Delete>** key.
2. Choose the MAC address that you want to delete and then press "**Enter**".
3. When pressing "**Enter**" will complete deletion.

■ Filtering MAC Address

You can add, delete, and edit filtering MAC address.

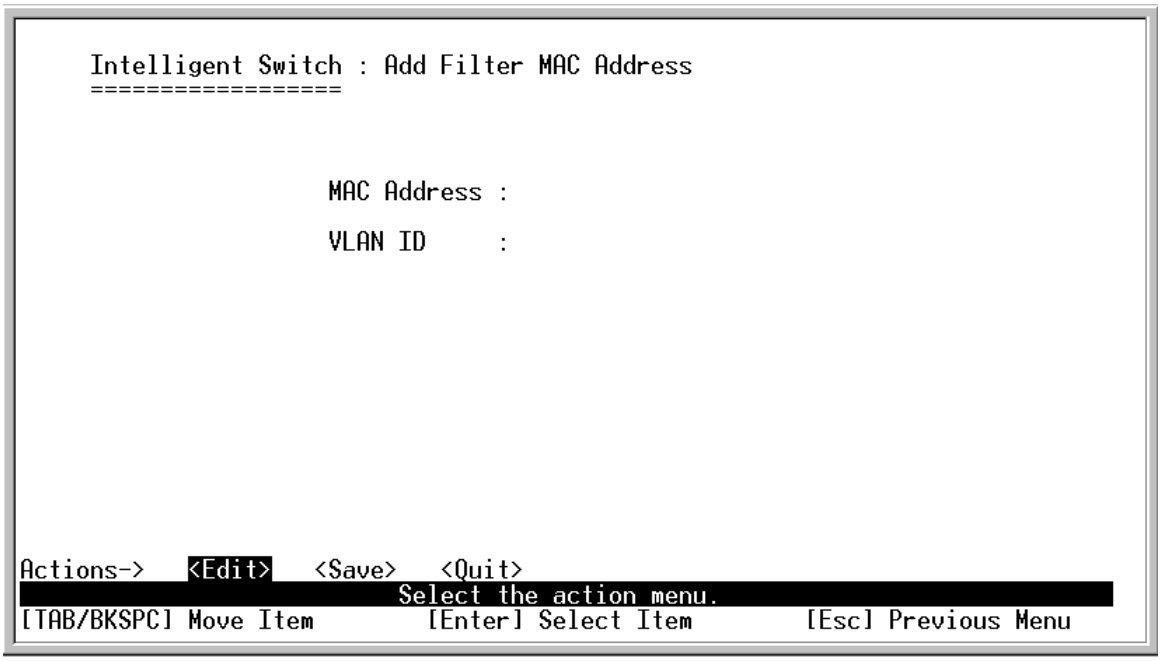


Add the Filtering MAC Address

1. Select **<Add>** → **<Edit>** key to add the static MAC address.

2. **MAC Address:** Enter the MAC address that you want to filter.
3. **VLAN ID:** Enter the Mac address's VLAN ID, if the Mac address belongs to any VLAN group.

   Note: if user does not do any VLAN configuration in advance, the setting of VALN ID will not showed in the screen.
4. Press "**ESC**" to go back action menu line.
5. Select **<Save>** to save all configure value.


Intelligent Switch : Add Filter MAC Address
MAC Address :
VLAN ID :
Actions-> <Edit> <Save> <Quit>
Select the action menu.
[TAB/BKSPC] Move Item [Enter] Select Item [Esc] Previous Menu

Edit Filtering MAC address

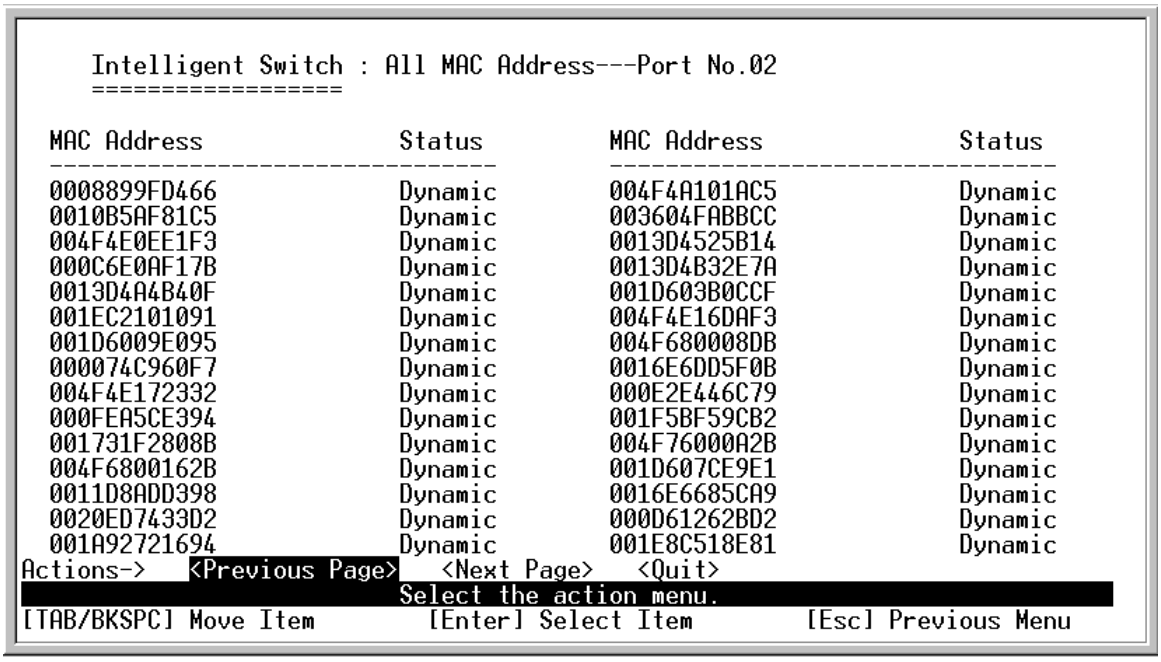
1. Select **<Edit>** key to modify a static Filtering address.
2. Choose the MAC address that you want to modify and then press "**Enter**".
3. Select **<Edit>** key to modify.
4. Press "**ESC**" to go back action menu line
5. Select **<Save>** to save all configure value.

Delete Filtering MAC address

1. Select **<Delete>** key to delete a Filtering MAC address.
2. Choose the MAC address that you want to delete and then press "**Enter**".
3. After delete Filtering MAC address, you have to select **<Save>** to complete the deleting operation.

- **All MAC Address**

1. Select **<Select>** key to select a port.
2. Press "**Space**" key to select the priority number and then press "**Enter**".
3. The current static & dynamic MAC address information of the port will be displayed.


Intelligent Switch : All MAC Address---Port No.02
MAC Address Status MAC Address Status
0008899FD466 Dynamic 004F4A101AC5 Dynamic
0010B5AF81C5 Dynamic 003604FABBCC Dynamic
004F4E0EE1F3 Dynamic 0013D4525B14 Dynamic
000C6E0AF17B Dynamic 0013D4B32E7A Dynamic
0013D4A4B40F Dynamic 001D603B0CCF Dynamic
001EC2101091 Dynamic 004F4E16DAF3 Dynamic
001D6009E095 Dynamic 004F680008DB Dynamic
000074C960F7 Dynamic 0016E6DD5F0B Dynamic
004F4E172332 Dynamic 000E2E446C79 Dynamic
000FEA5CE394 Dynamic 001F5BF59CB2 Dynamic
001731F2808B Dynamic 004F76000A2B Dynamic
004F6800162B Dynamic 001D607CE9E1 Dynamic
0011D8ADD398 Dynamic 0016E6685CA9 Dynamic
0020ED7433D2 Dynamic 000D61262BD2 Dynamic
001A92721694 Dynamic 001E8C518E81 Dynamic
Actions-> <Previous Page> <Next Page> <Quit>
Select the action menu.
[TAB/BKSPC] Move Item [Enter] Select Item [Esc] Previous Menu

Misc Configuration

You can configure the switch parameters and stacking function. The stacking function provides you can centralize the control of the switch in the network. For the manager personal, he/she can save the time and easily on switches controlling.

- **MAC Address Ageing Time:** MAC address table refresh time setting. Type the number of seconds that an inactive MAC address remains in the switch's address table. The valid range is 0, 300~765 seconds. Default is 300 seconds.
- **Broadcast Storm Filter mode:** configure the broadcast storm filter mode. The valid threshold values are 5%, 10%, 15%, 20%, 25%, and N/A. The port will be block cause of broadcast packet is over the percentage of traffic.
- **Max Bridge Transmit Delay Bound:** Limit the packets queuing time in switch. If

enable, the packets queued exceed will be drop. Press **Space** key to set the time. This valid value is 1sec, 2sec, 4sec and off. Default is off.

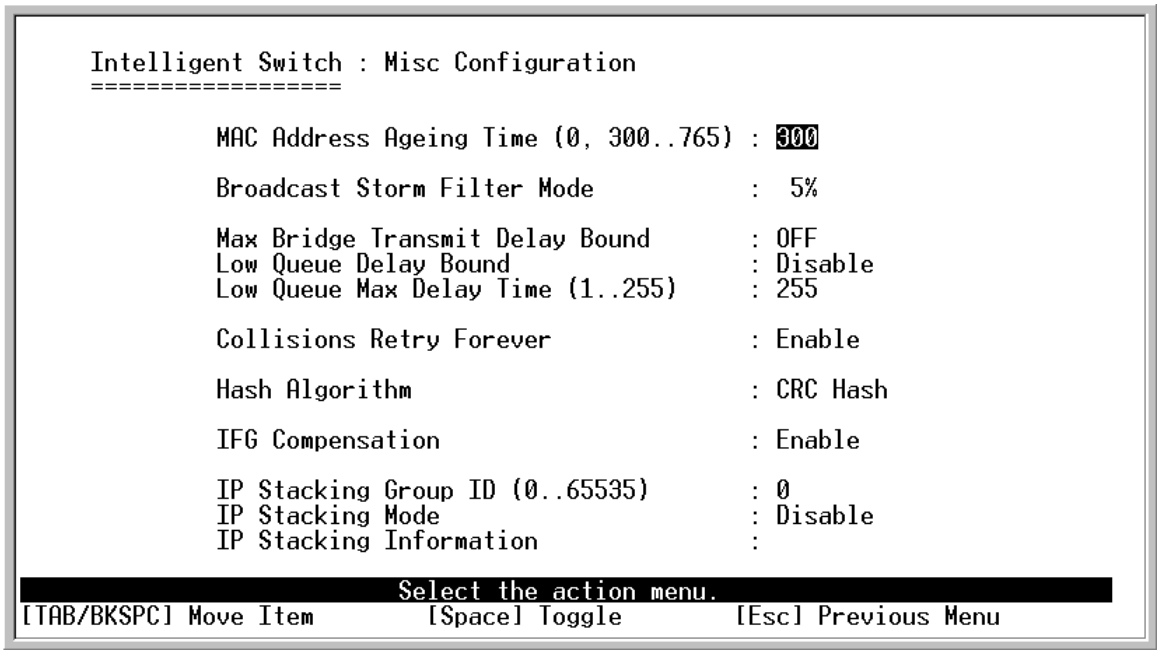
- **Low Queue Delay Bound:** Limit the low priority packets queuing time in switch. If enable, the low priority packet stays in switch exceed Low Queue Max Delay Time, it will be sent. Press **Space** key to enable or disable this function.
- **Low Queue Max Delay Time:** To set the time that low priority packets queuing in switch. Default Max Delay Time is 255ms. The valid range is 1~255 ms.

NOTE: Make sure of "Max bridge transit delay bound control" is enabled before enable Low Queue Delay Bound, because Low Queue Delay Bound must be work under "Max bridge transit delay bound control" is enabled situation.

- **Collisions Retry Forever:** Disable – In half duplex, if happens collision, the switch will retry 48 times and then drop frame. Enable – In half duplex, if happens collision, the switch will retry forever
- **Hash Algorithm:** This Hash Algorithm is for hardware maintaining on MAC table calculation. Provide CRC or Direct Map
- **IFG compensation:** Disable or Enable
- **IP Stacking Group ID (0…65535):** assign the stacking group ID. The switches must assign the same stacking group ID to be stacked as a group.
- **IP Stacking Mode:** enabling/disabling the stacking function. There are three stacking modes. Any port on the switch can be used to stack. To configure the switch in stacking group, please use the Web GUI configuration interface.
  - **Disable:** The stacking function is not working.
  - **Master:** There must have a leader switch to control all other switches in stacking group. You can only assign one switch to be the master switch in one stacking group. When the stacking group is set up, the master switch will control all switches in the stacking group.
  - **Slave:** besides the master switch, rest of the switches are called slave switch in stacking group. When the stacking group is set up, you can only configure the slave switches through the master switch.

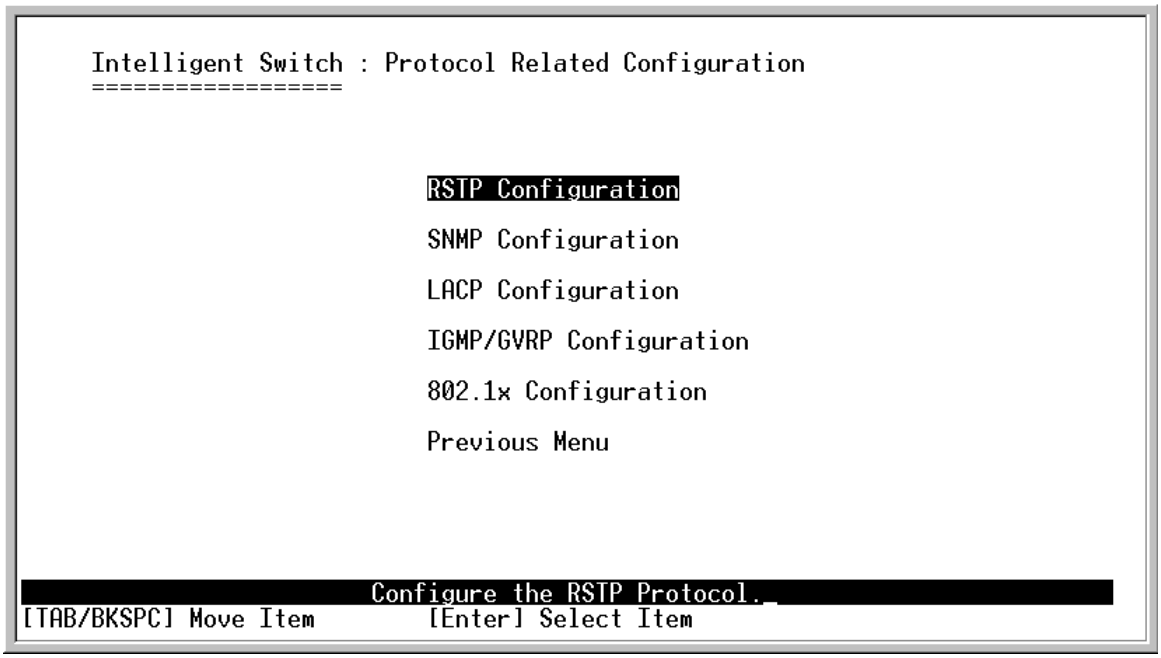
Note:

1. Before configuring the stacking function, make sure all stack switches are in the same network.
2. Configure stacking function; you must configure the master switch first.
3. After you have configured the stacking function, use Cat. 5 cable to connect every switch in the stacking group.
4. To remove the switch from stacking group, you must remove the salve switch first. When all slave switches are removed, you can remove the master switch from stacking group.


Intelligent Switch : Misc Configuration
MAC Address Ageing Time (0, 300..765) : 300
Broadcast Storm Filter Mode : 5%
Max Bridge Transmit Delay Bound : OFF
Low Queue Delay Bound : Disable
Low Queue Max Delay Time (1..255) : 255
Collisions Retry Forever : Enable
Hash Algorithm : CRC Hash
IFG Compensation : Enable
IP Stacking Group ID (0..65535) : 0
IP Stacking Mode : Disable
IP Stacking Information :
Select the action menu.
[TAB/BKSPC] Move Item
[Space] Toggle
[Esc] Previous Menu

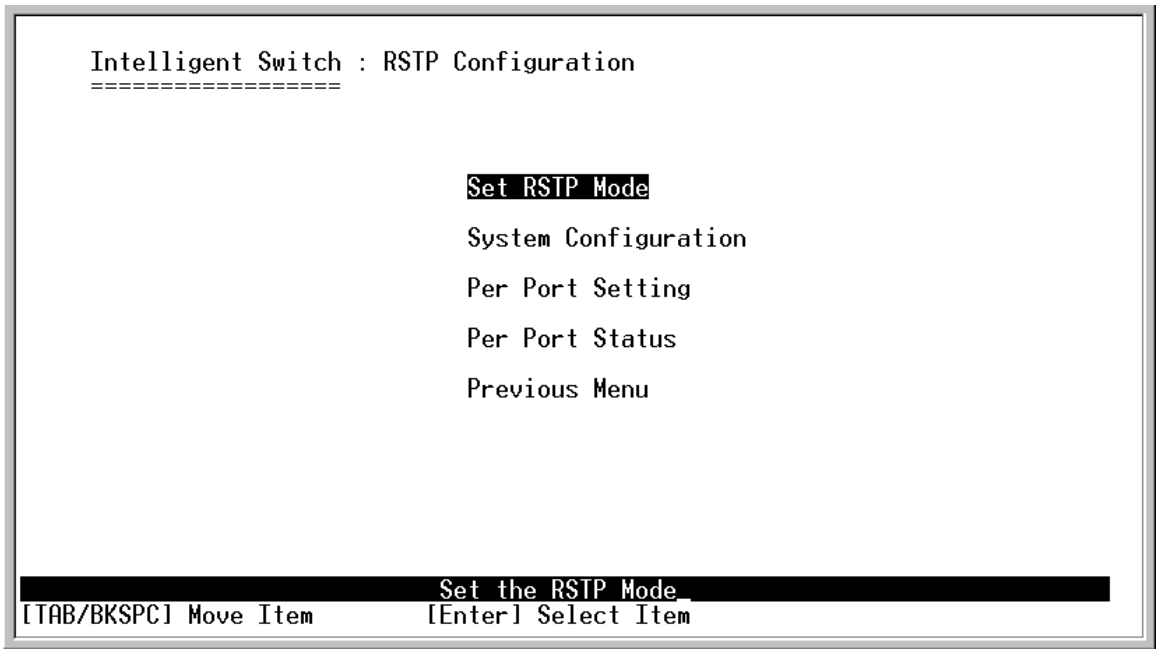
5.4.3 Protocol Related Configuration

You can configure Spanning Tree Protocol, SNMP, LACP, IGMP/GVRP, and 802.1x in Protocol Relate Configuration section.



RSTP

Spanning tree is a link management protocol that provides path redundancy while preventing undesirable loops in the network.



■ RSTP Setup

You must enable Rapid Spanning Tree function before configuring RSTP function.

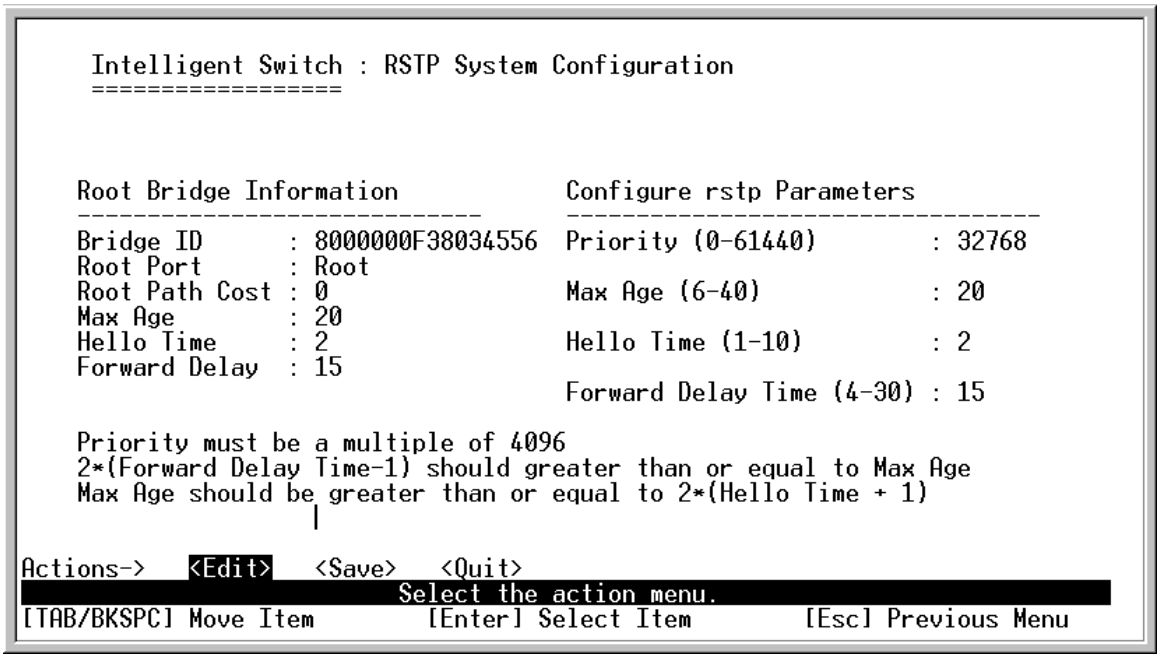
1. Select **<Edit>**
2. Use "**Space**" key to select the option. User can select "**RSTP**", "**Disable**" or "**STP**".
3. Select **<Save>**.

■ System Configuration

You can configure the RSTP system parameter after enable the RSTP function. You can view spanning tree information about the Root Bridge on the left.

1. Select **<Edit>**
2. **Priority:** Assign path priority number. The valid value is 0 ~ 61440. The default is 32678.
3. **Max Age:** The maximum path age. The valid value is 6 ~ 40 seconds. The default is 20 seconds.

4. **Hello Time:** The time that controls switch sends out the BPDU packet to check STP current status. The valid value is 1 ~ 10 seconds. The default is 2 seconds.
5. **Forward Delay Time:** forward delay time. The valid value is 4 ~ 30 seconds. The default is 15 seconds.
6. Select **<Save>**.


Intelligent Switch : RSTP System Configuration
Root Bridge Information
Bridge ID : 8000000F38034556
Root Port : Root
Root Path Cost : 0
Max Age : 20
Hello Time : 2
Forward Delay : 15
Configure rstp Parameters
Priority (0-61440) : 32768
Max Age (6-40) : 20
Hello Time (1-10) : 2
Forward Delay Time (4-30) : 15
Priority must be a multiple of 4096
2*(Forward Delay Time-1) should greater than or equal to Max Age
Max Age should be greater than or equal to 2*(Hello Time + 1)
Actions-> <Edit> <Save> <Quit>
Select the action menu.
[TAB/BKSPC] Move Item [Enter] Select Item [Esc] Previous Menu

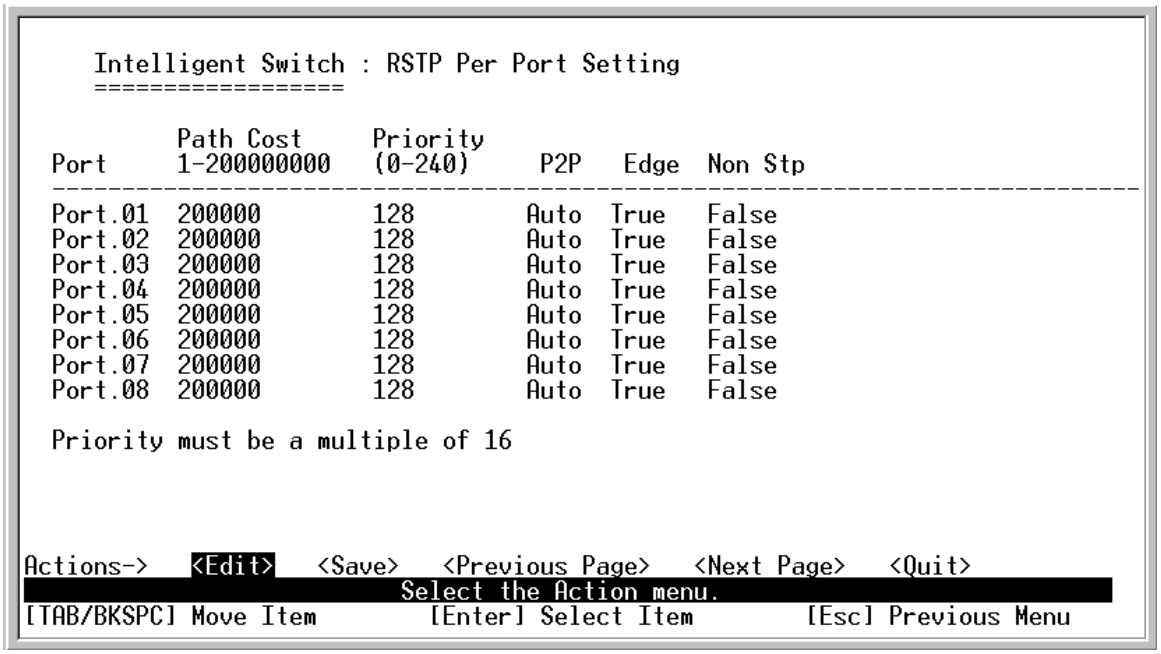
- **Per Port Setting**

1. Select **<Edit>**.
2. **Path Cost:** specifies the path cost of the port that switch uses to determine which port are the forwarding ports. The value range is from 1 to 65535. The default is 20000.
3. **Priority:** It means port priority; you can make it more or less likely to become the root port. The valid value is from 0 to 255. The lowest value has higher priority. The default is 128.

- **Admin P2P:** There are three parameters, Auto, True and False, used to configure the type of the point-to-point link. If configuring this parameter to be Auto, it means RSTP will use the duplex mode resulted from the auto-negotiation. In today's switched networks, most links are running in full-duplex mode. For sure, the result may be half-duplex, in this case, the port will not fast transit to Forwarding state. If it is set as True, the port is treated as point-to-point link by RSTP and unconditionally transited to Forwarding state. If it is set as False, fast transition to Forwarding state will not happen on this port. The default is Auto.
- **Admin Edge**: If user selects "True", this port will be an edge port. An Edge Port is a port

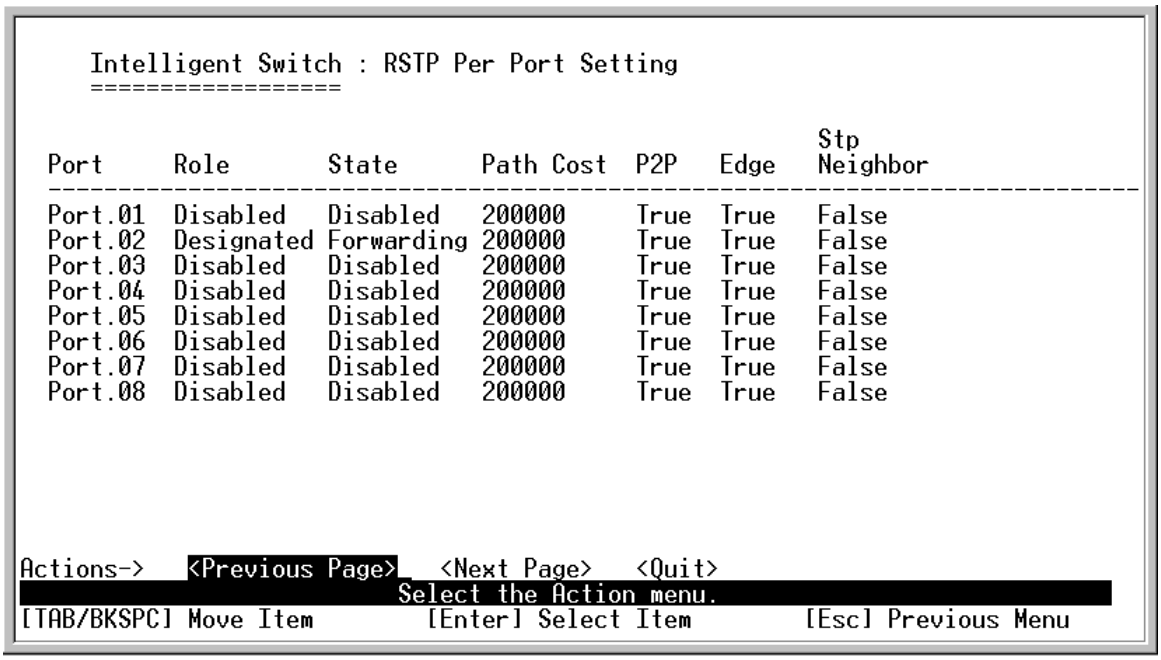
connected to a device that knows nothing about STP or RSTP. Usually, the connected device is an end station. Edge Ports will immediately transit to forwarding state and skip the listening and learning state because the edge ports cannot create bridging loops in the network. This will expedite the convergence. When the link on the edge port toggles, the STP topology keeps unchanged. Unlike the designate port or root port though, an edge port will transit to a normal spanning-tree port immediately if it receives a BPDU. The default is True.

4. **Admin Non Stp**: The port includes the STP mathematic calculation. True is not including STP mathematic calculation. False is including the STP mathematic calculation. The default is False.
5. Press "**ESC**" goes back action menu line.
6. Select **<Save>** to save all configure value.
7. On the action menu line you can press **<Next Page>** to configure port9 ~ port26, press **<Previous Page>** return to previous page.


Intelligent Switch : RSTP Per Port Setting
Path Cost
Priority
Port
1-200000000
(0-240)
P2P
Edge
Non Stp
Port.01 200000 128 Auto True False
Port.02 200000 128 Auto True False
Port.03 200000 128 Auto True False
Port.04 200000 128 Auto True False
Port.05 200000 128 Auto True False
Port.06 200000 128 Auto True False
Port.07 200000 128 Auto True False
Port.08 200000 128 Auto True False
Priority must be a multiple of 16
Actions-> <Edit> <Save> <Previous Page> <Next Page> <Quit>
Select the Action menu.
[TAB/BKSPC] Move Item [Enter] Select Item [Esc] Previous Menu

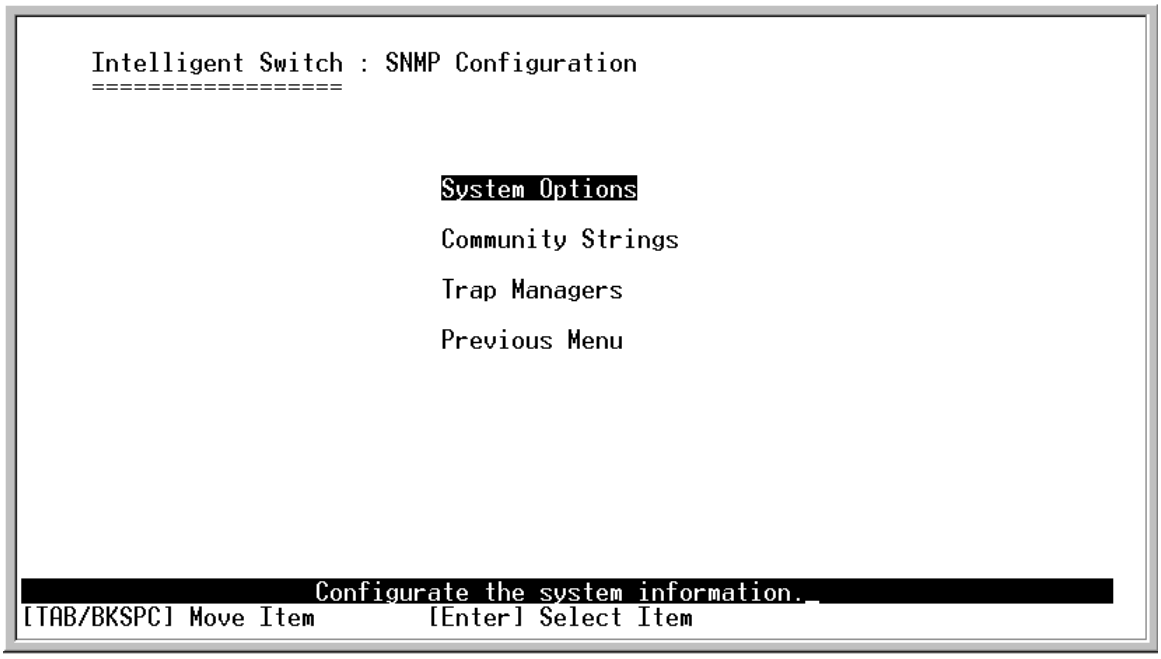
- **Per Port Status**

It will display the status of every port.


Intelligent Switch : RSTP Per Port Setting
Port Role State Path Cost P2P Edge Stp Neighbor
Port.01 Disabled Disabled 200000 True True False
Port.02 Designated Forwarding 200000 True True False
Port.03 Disabled Disabled 200000 True True False
Port.04 Disabled Disabled 200000 True True False
Port.05 Disabled Disabled 200000 True True False
Port.06 Disabled Disabled 200000 True True False
Port.07 Disabled Disabled 200000 True True False
Port.08 Disabled Disabled 200000 True True False
Actions-> <Previous Page> <Next Page> <Quit>
Select the Action menu.
[TAB/BKSPC] Move Item [Enter] Select Item [Esc] Previous Menu

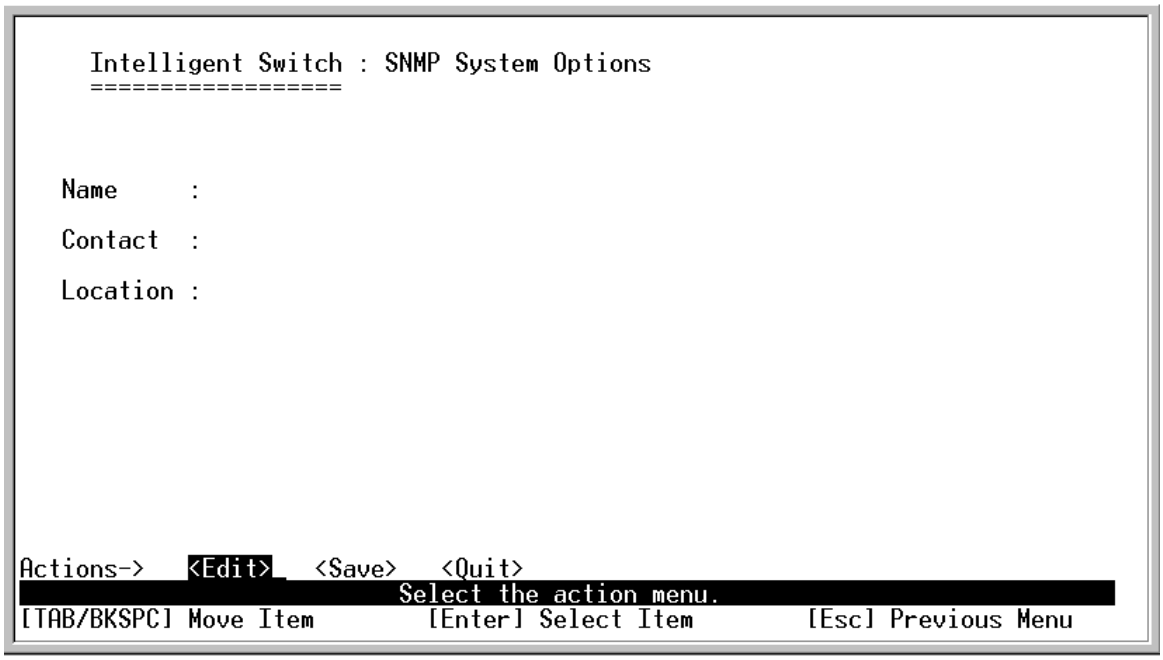
SNMP

To define management stations as trap managers and to enter SNMP community strings. You can also define a name, location, and contact person for the switch.



■ SNMP System Options

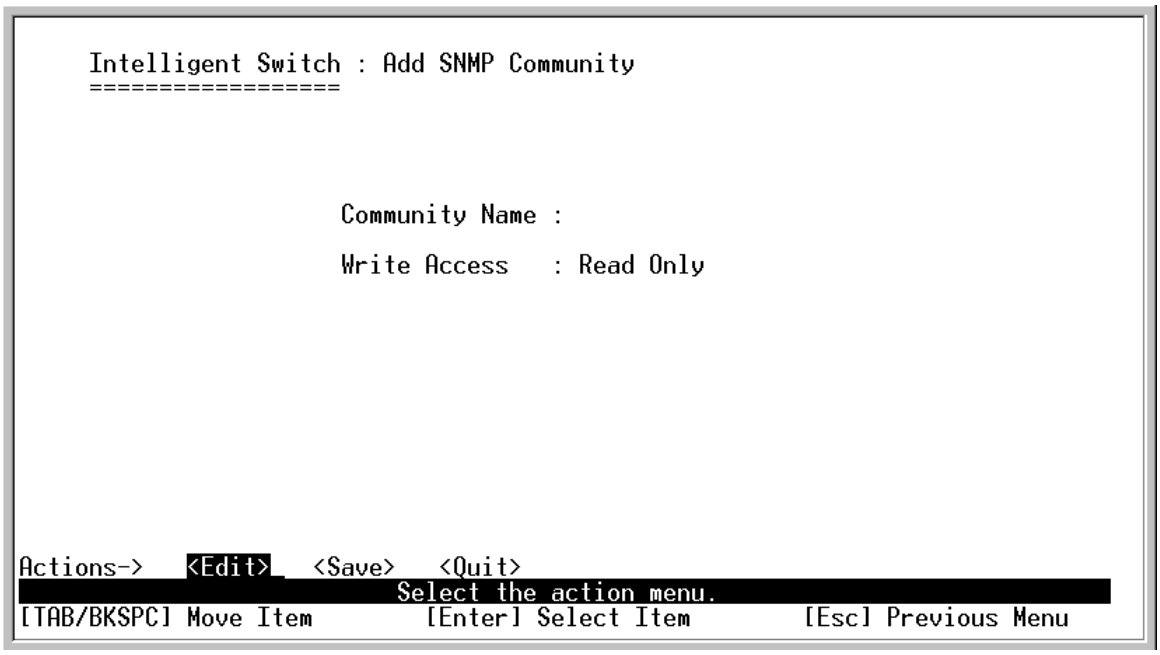
1. Press **<Edit>**.
2. **System Name:** assign a name for the switch.
3. **System Contact:** Type the name of contact person or organization.
4. **System Location:** Type the location of the switch.
5. Press "**ESC**" goes back action menu line.
6. Press **<Save>** to save configured value.



■ Community Strings

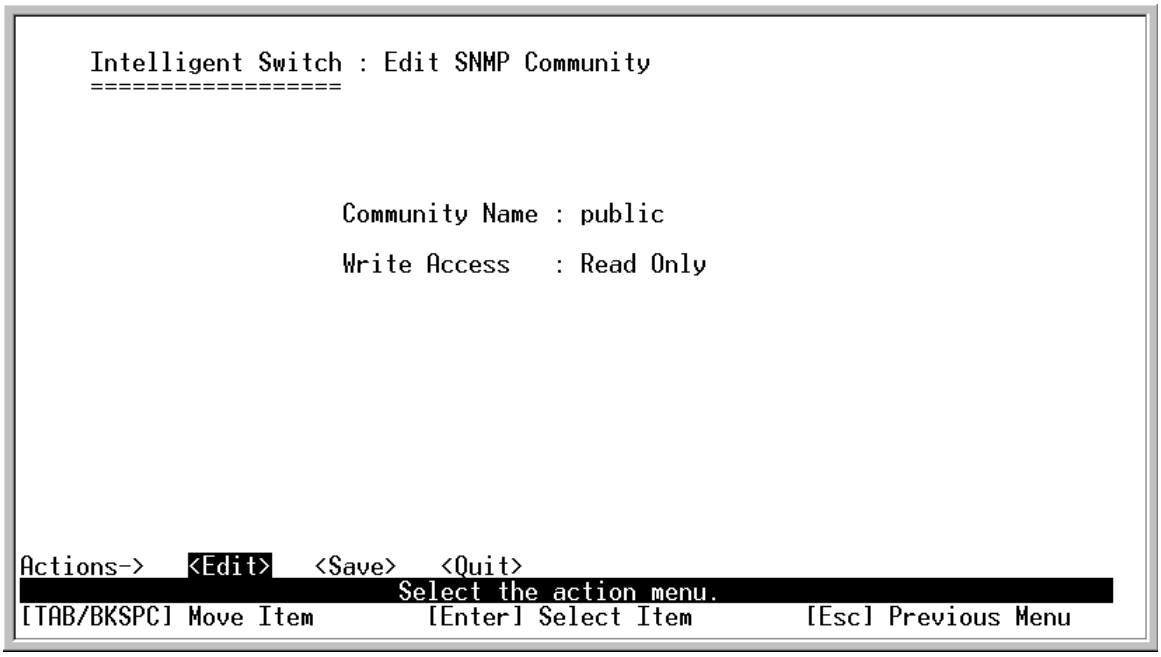
Add Community Strings

1. Select **<Add>**
2. Select **<Edit>**
3. **Community Name:** Type the name of community strings.
4. **Write Access:** Enable the rights is read only or read/write.
   - **Read only:** Read only, enables requests accompanied by this string to display MIB-object information.
   - **Read/Write:** Read write, enables requests accompanied by this string to display MIB-object information and to set MIB objects.


Intelligent Switch : Add SNMP Community
Community Name :
Write Access : Read Only
Actions-> <Edit> <Save> <Quit>
Select the action menu.
[TAB/BKSPC] Move Item [Enter] Select Item [Esc] Previous Menu

Edit Community Name

1. Select **<Edit>**
2. Choose the item that you want to modify and then press "**Enter**"**.**
3. **Community Name:** type the new name.
4. **Write Access:** Press "**Space**" key to change the right.
5. Select **<Save>**.

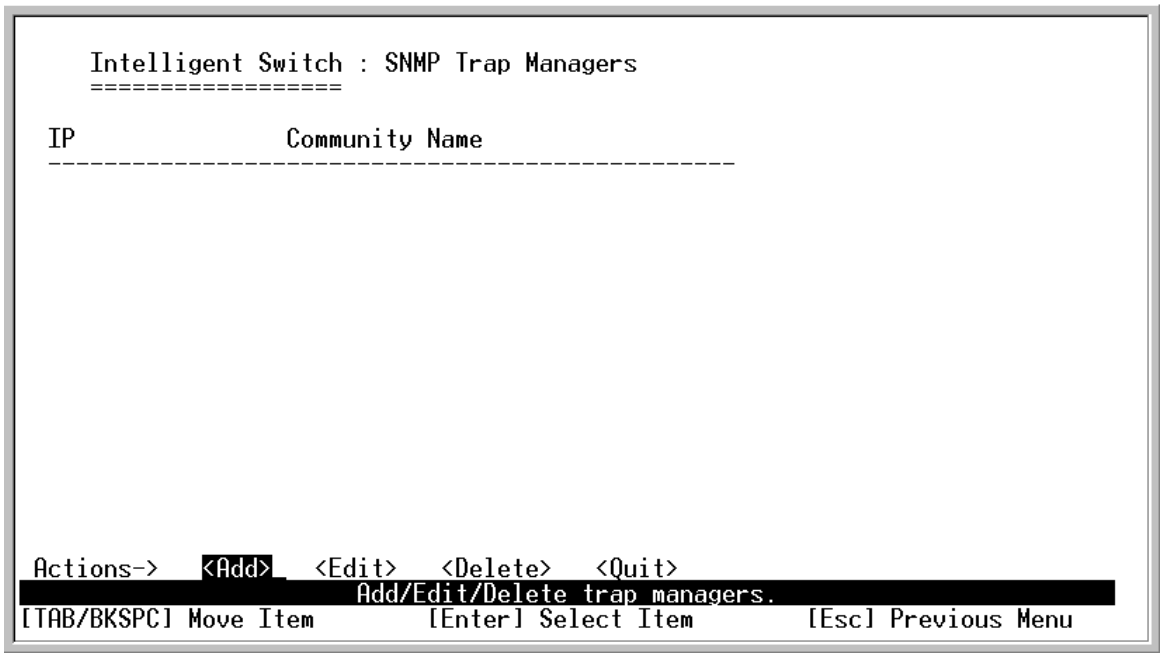

Intelligent Switch : Edit SNMP Community
Community Name : public
Write Access : Read Only
Actions-> <Edit> <Save> <Quit>
Select the action menu.
[TAB/BKSPC] Move Item [Enter] Select Item [Esc] Previous Menu

Delete Community Name

1. Select **<Delete>**.
2. Choose the community name that you want to delete and then press "**Enter**".

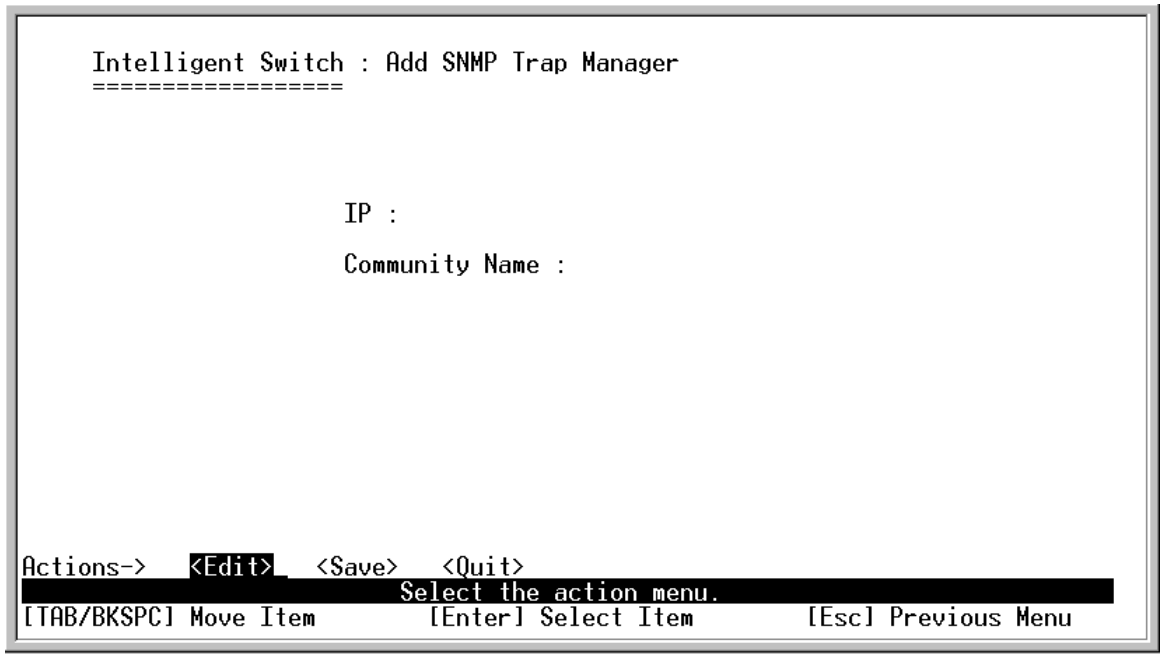
■ Trap Managers

A trap manager is a management station that receives traps, the system alerts generated by the switch. If no trap manager is defined, no traps will issue. Create a trap manager by entering the IP address of the station and a community string.



Add the trap manager

1. Select **<Add>** → **<Edit>** to add the trap manager.
2. **IP:** enter the IP address of trap manager.
3. **Community Name:** enter the community string.
4. Press "**ESC**" go back to actions menu line
5. Select **<Save>** to save all configure.

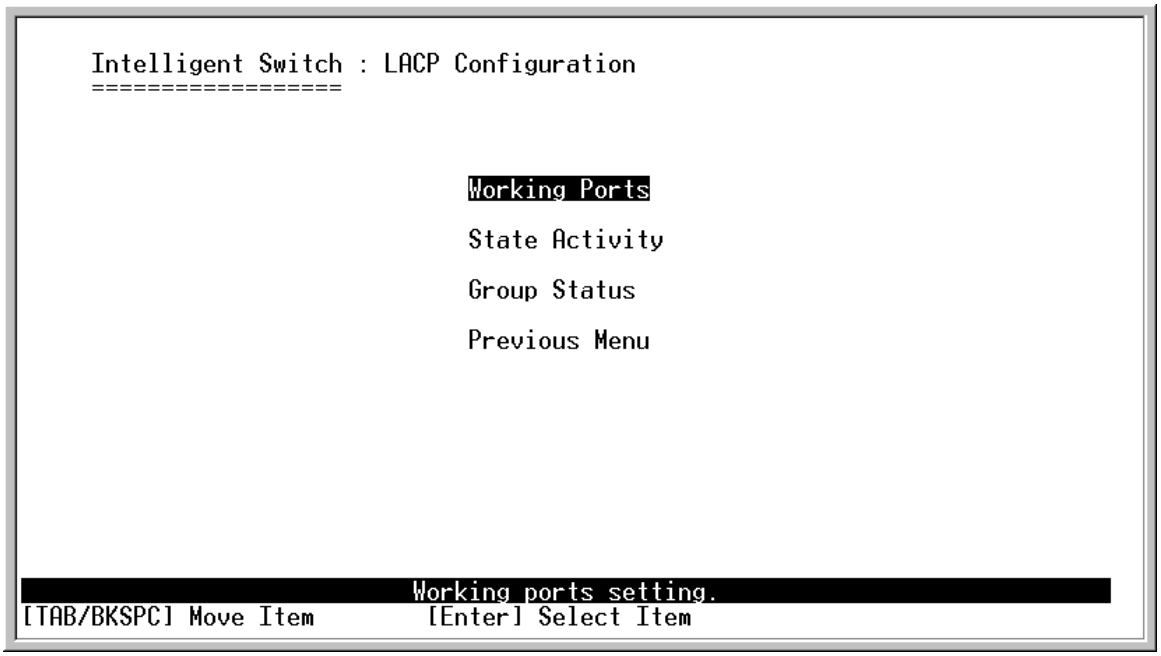


Delete Trap Manager

1. Select **<Delete>**
2. Choose the trap manager that you want to delete and then press "**Enter**".

LACP

The Link Aggregation Control Protocol (LACP) provides a standardized means for exchanging information between Partner Systems on a link to allow their Link Aggregation Control instances to reach agreement on the identity of the Link Aggregation Group to which the link belongs, move the link to that Link Aggregation Group, and enable its transmission and reception functions in an orderly manner. Link aggregation lets you group up to eight consecutive ports into a single dedicated connection. This feature can expand bandwidth to a device on the network. **LACP operation requires full-duplex mode,** more detail information refers to IEEE 802.3ad.



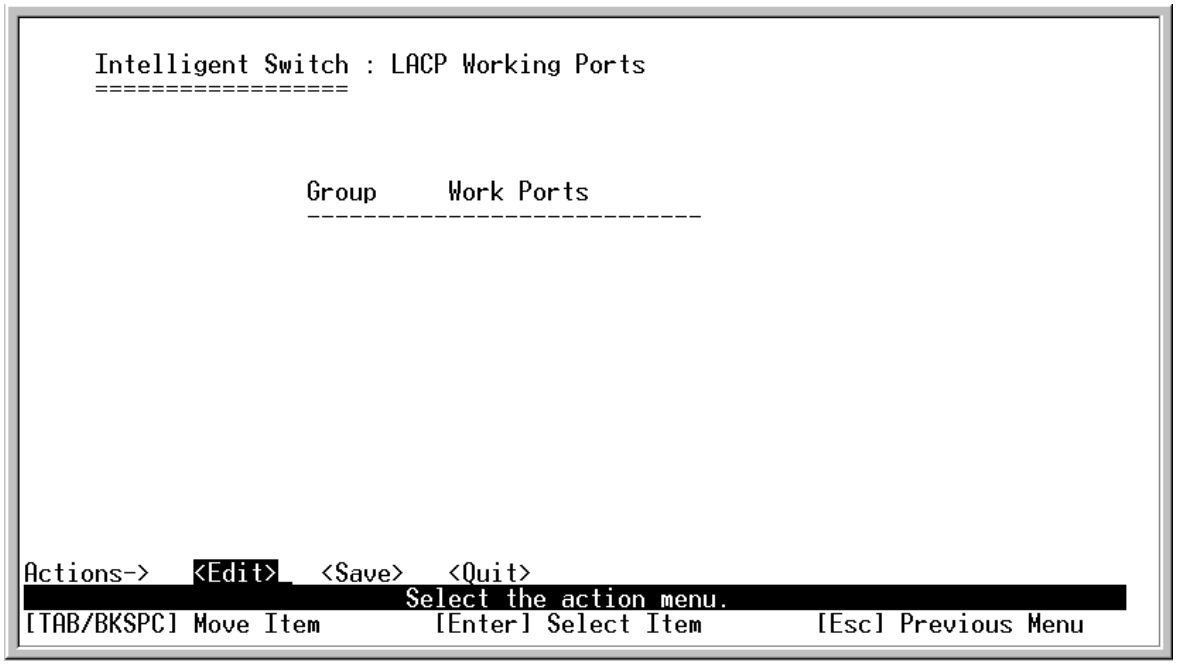
- **Working Port Setting**

1. Select **<Edit>**
2. **Group:** Display the trunk group ID.
3. **LACP:** Press "**Space**" key to enable or disable LACP (Link Aggregation Control Protocol) support. When LACP enable, the group is LACP static trunk group. When

LACP disable, the group is local static trunk group.

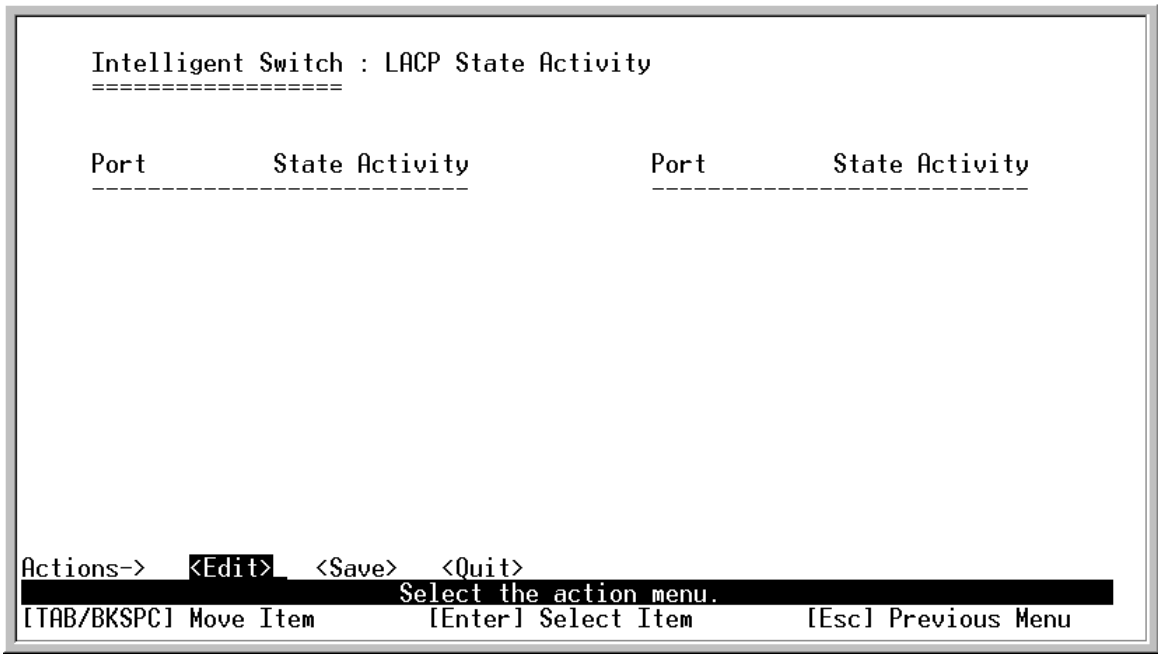
4. **Working Port Num:** The max number of ports can be aggregated at the same time. If LACP static trunk group, the exceed ports is standby and able to aggregate if work ports fail. If it is local static trunk group, the number must be the same as group ports.
5. Select **<Save>**

   NOTE: Before set LACP support, you have to set trunk group on the Trunk Configuration.



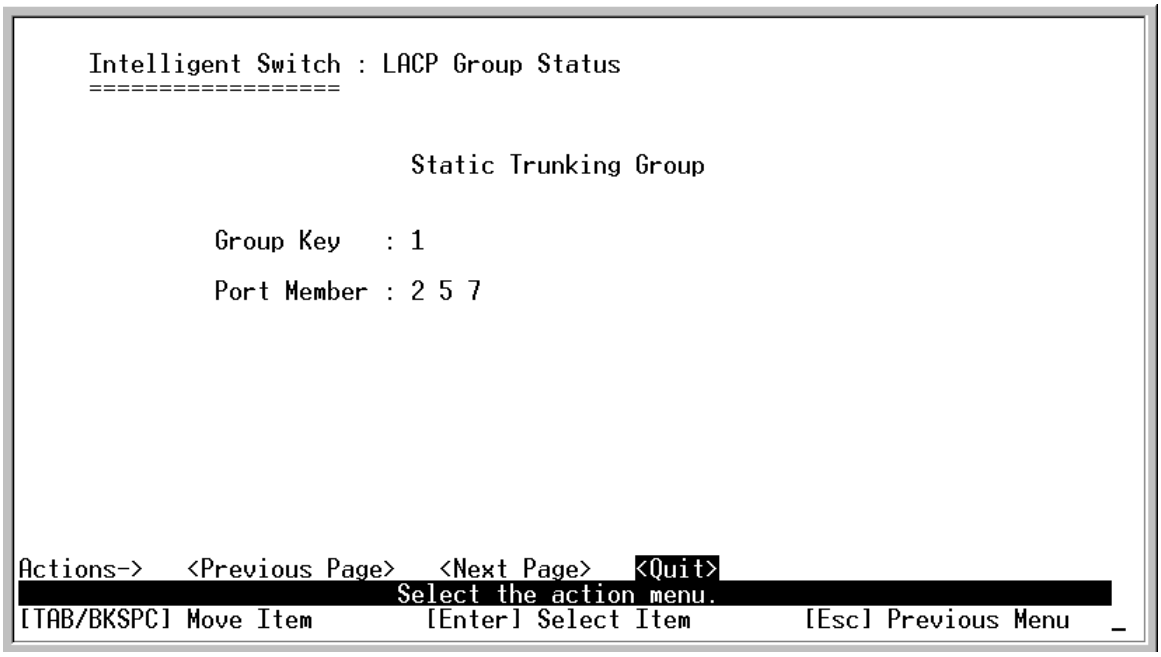
- **LACP State Activity**

1. Select **<Edit>**
2. Use "**Space**" key to select the Port State Activity.
   - **Active:** The port automatically sends LACP protocol packets.
   - **Passive:** The port does not automatically send LACP protocol packets, and responds only if it receives LACP protocol packets from the opposite device.
3. Select **<Save>**.



■ Group Status

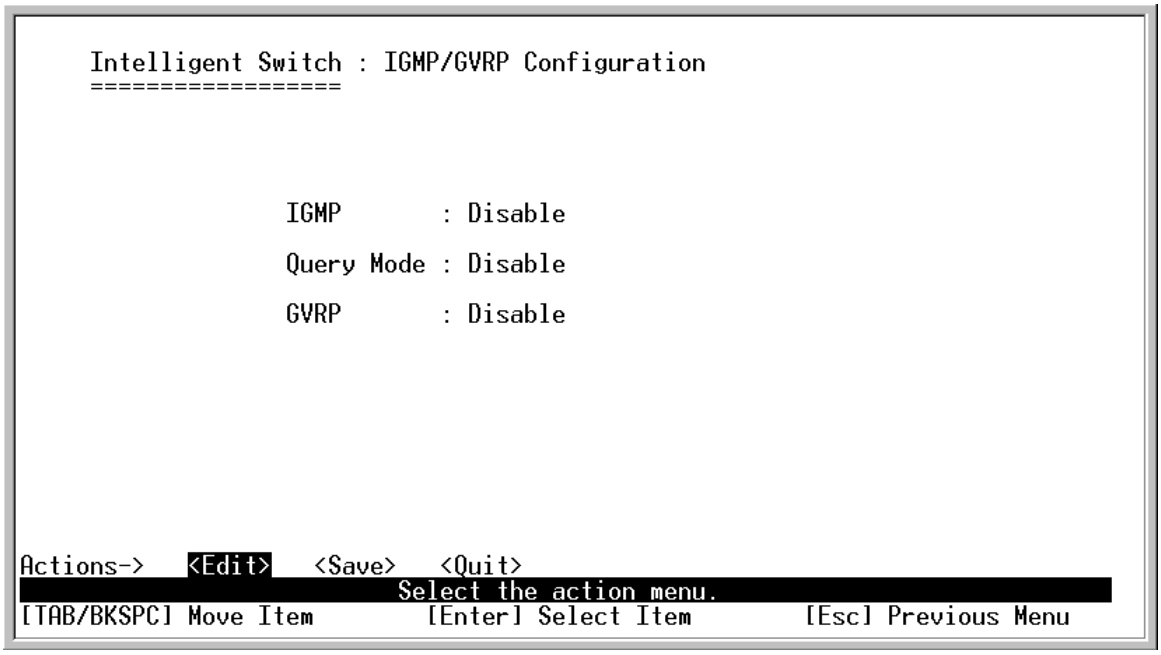
When setting trunk group, you can see the relation information in here.



IGMP/GVRP

You can enable or disable the IGMP/GVRP (GARP VLAN Registration Protocol).

1. Select **<Edit>**
2. Use "**Space**" key to change the value
3. Select **<Save>**


Intelligent Switch : IGMP/GVRP Configuration
IGMP : Disable
Query Mode : Disable
GVRP : Disable
Actions-> <Edit> <Save> <Quit>
Select the action menu.
[TAB/BKSPC] Move Item [Enter] Select Item [Esc] Previous Menu

802.1x Configuration

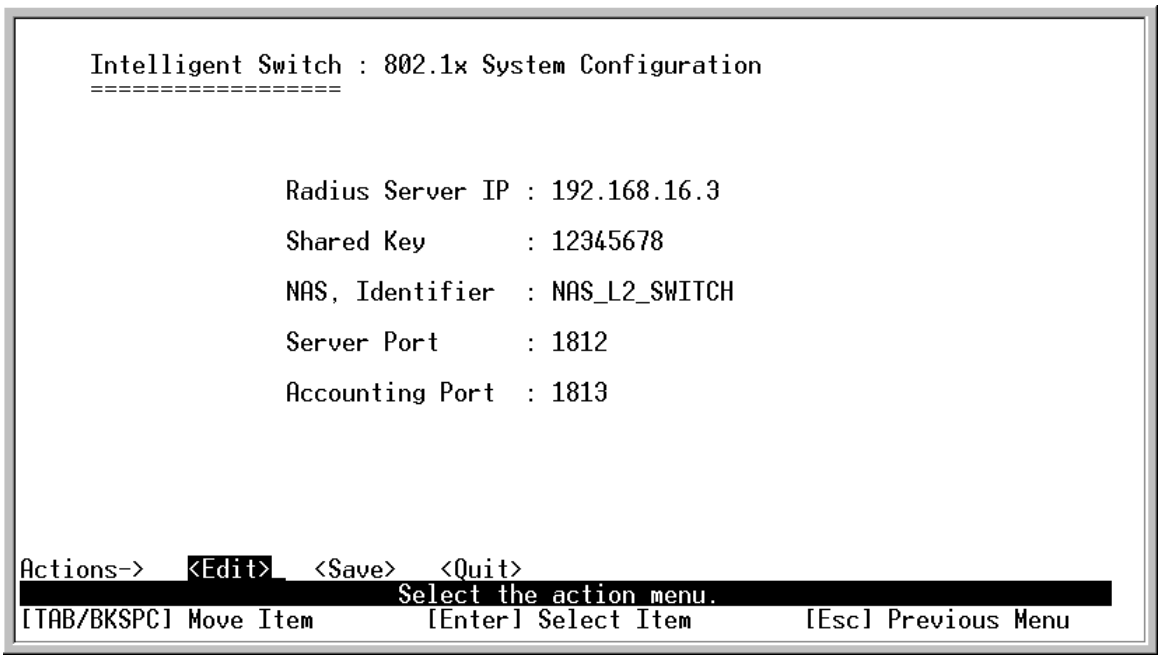
802.1x Setup

1. Select **<Edit>**
2. Use "**Space**" key to Enable or Disable the 802.1x.
3. Select **<Save>**

System Configuration

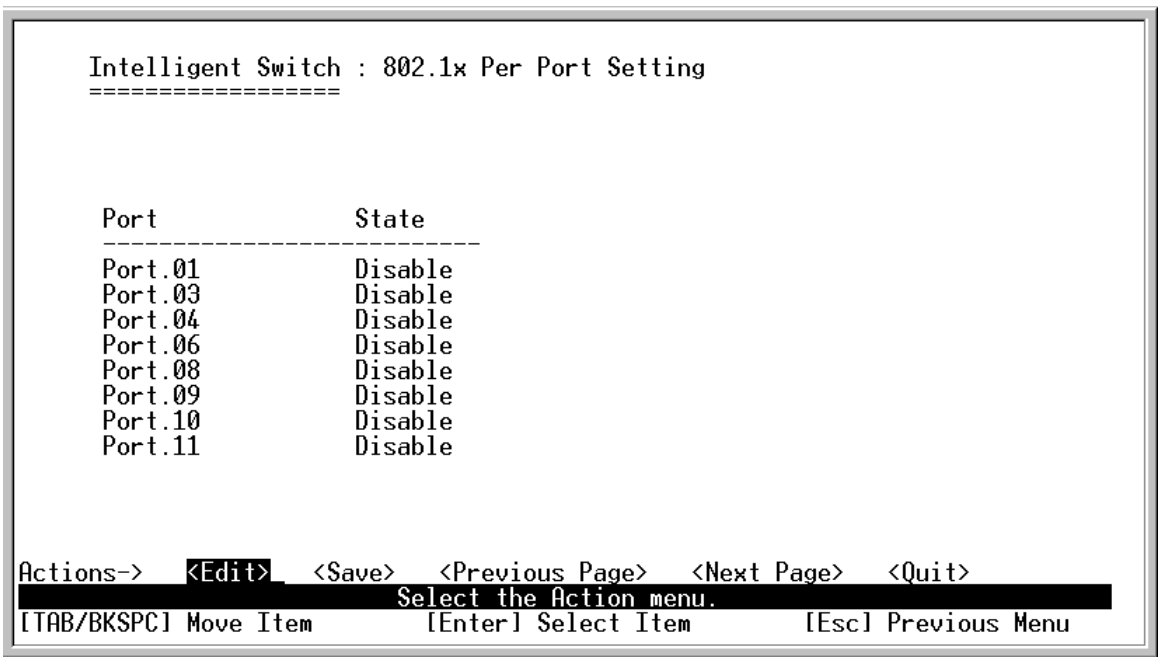
After enabling the IEEE 802.1x function, you can configure the parameters of this function.

1. Select **<Edit>**.
2. **Radius Server IP:** set the Radius Server IP address.
3. **Shared Key:** set an encryption key for using during authentication sessions with the specified radius server. This key must match the encryption key used on the Radius Server.
4. **NAS, Identifier:** set the identifier for the radius client.
5. **Server Port:** set the UDP destination port for authentication requests to the specified Radius Server.
6. **Accounting Port:** set the UDP destination port for accounting requests to the specified Radius Server.
7. Select **<Save>**.


Intelligent Switch : 802.1x System Configuration
Radius Server IP : 192.168.16.3
Shared Key : 12345678
NAS, Identifier : NAS_L2_SWITCH
Server Port : 1812
Accounting Port : 1813
Actions-> <Edit> <Save> <Quit>
Select the action menu.
[TAB/BKSPC] Move Item [Enter] Select Item [Esc] Previous Menu

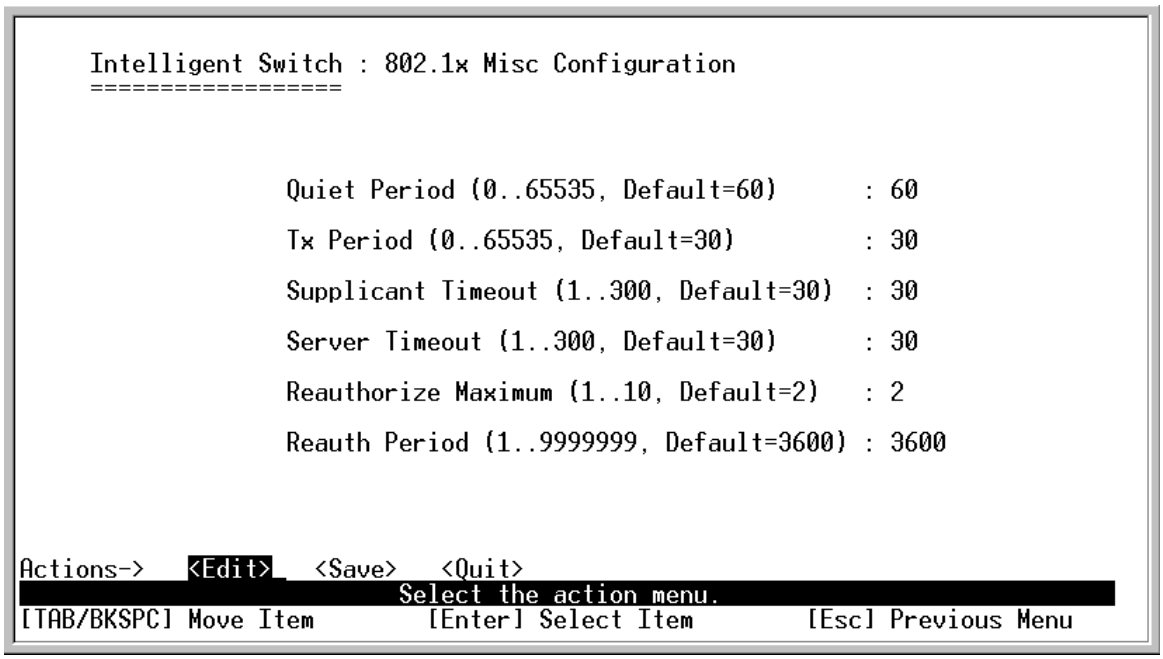
■ Per Port Configuration

You can configure 802.1x authentication state for each port. The State provides Disable, Accept, Reject and Authorize. Use "**Space**" key to change the state value.



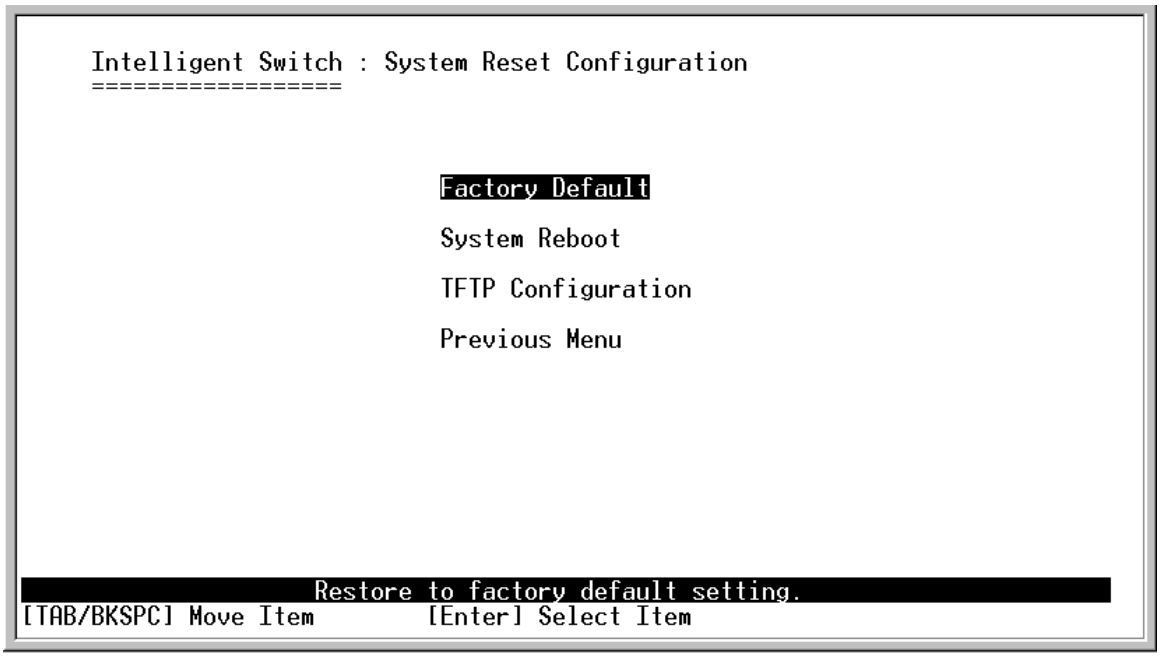
- **Misc Configuration**

1. Select **<Edit>**
2. **Quiet Period:** set the period during which the port doesn't try to acquire a supplicant.
3. **TX Period:** set the period the port wait for retransmit next EAPOL PDU during an authentication session.
4. **Supplicant Timeout:** set the period of time the switch waits for a supplicant response to an EAP request.
5. **Server Timeout:** set the period of time the switch waits for a server response to an authentication request.
6. **Reauthorize Maximum:** set the number of authentication that must time-out before authentication fails and the authentication session ends.
7. **Reauthorize period:** set the period of time after which clients connected must be re-authenticated.
8. Select **<Save>**


Intelligent Switch : 802.1x Misc Configuration
Quiet Period (0..65535, Default=60) : 60
Tx Period (0..65535, Default=30) : 30
Supplicant Timeout (1..300, Default=30) : 30
Server Timeout (1..300, Default=30) : 30
Reauthorize Maximum (1..10, Default=2) : 2
Reauth Period (1..9999999, Default=3600) : 3600
Actions-> <Edit> <Save> <Quit>
Select the action menu.
[TAB/BKSPC] Move Item [Enter] Select Item [Esc] Previous Menu

5.4.4 System Reset Configuration

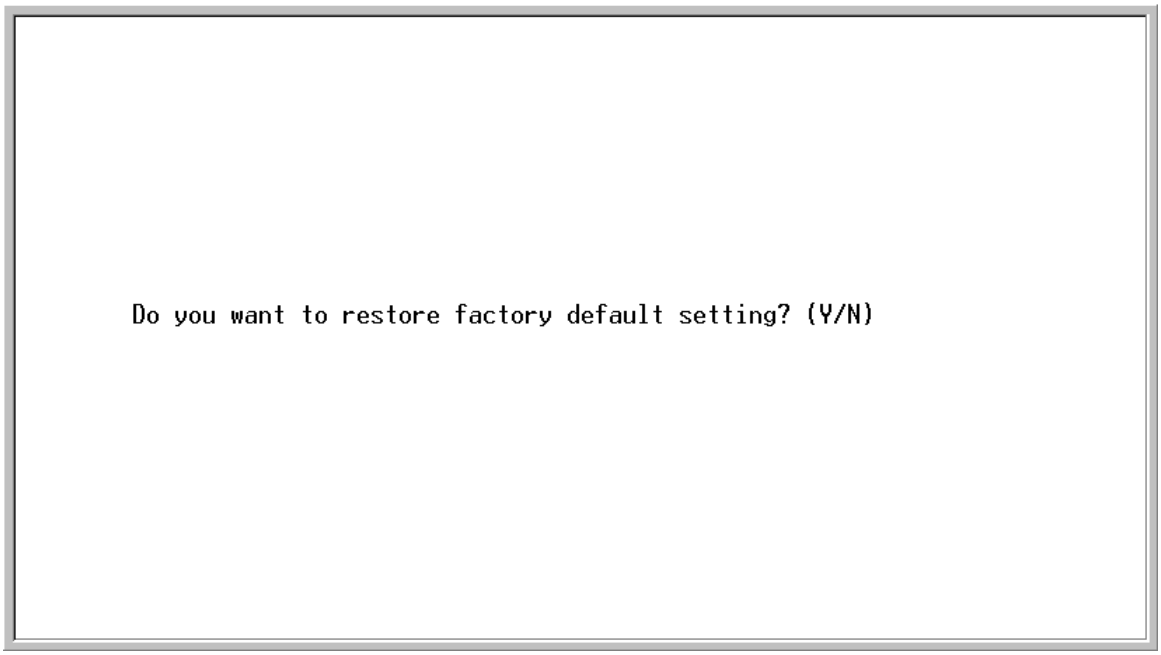
You can reset the system back to default value, reboot the system and update the system firmware.



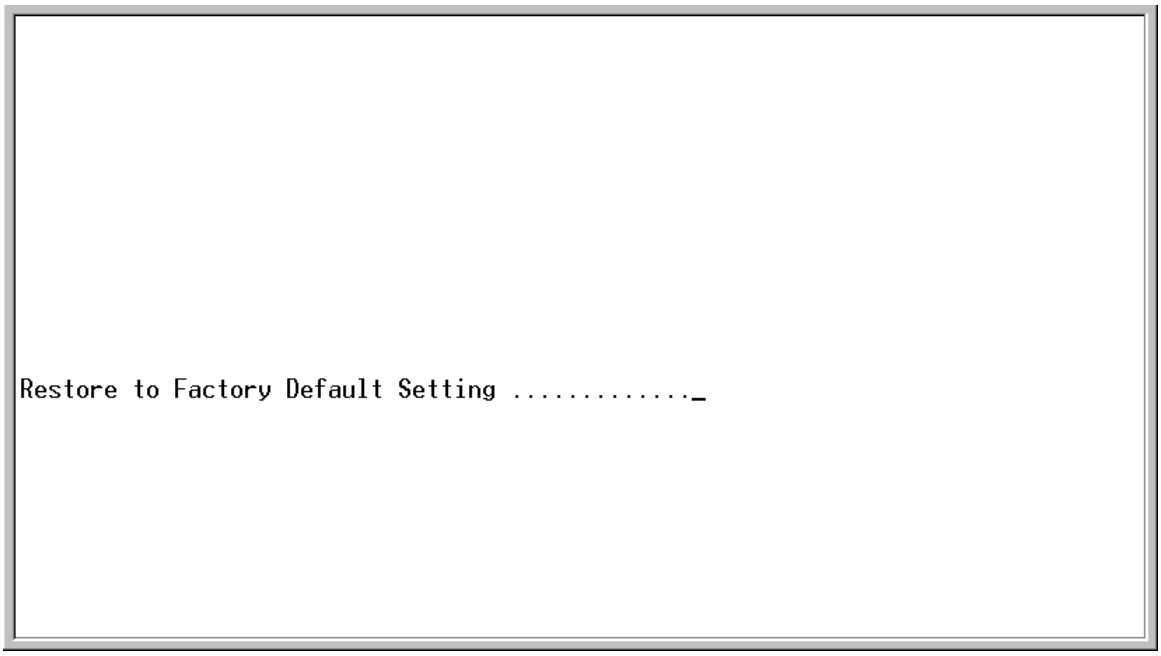
Factory Default

Reset switch to default configuration.

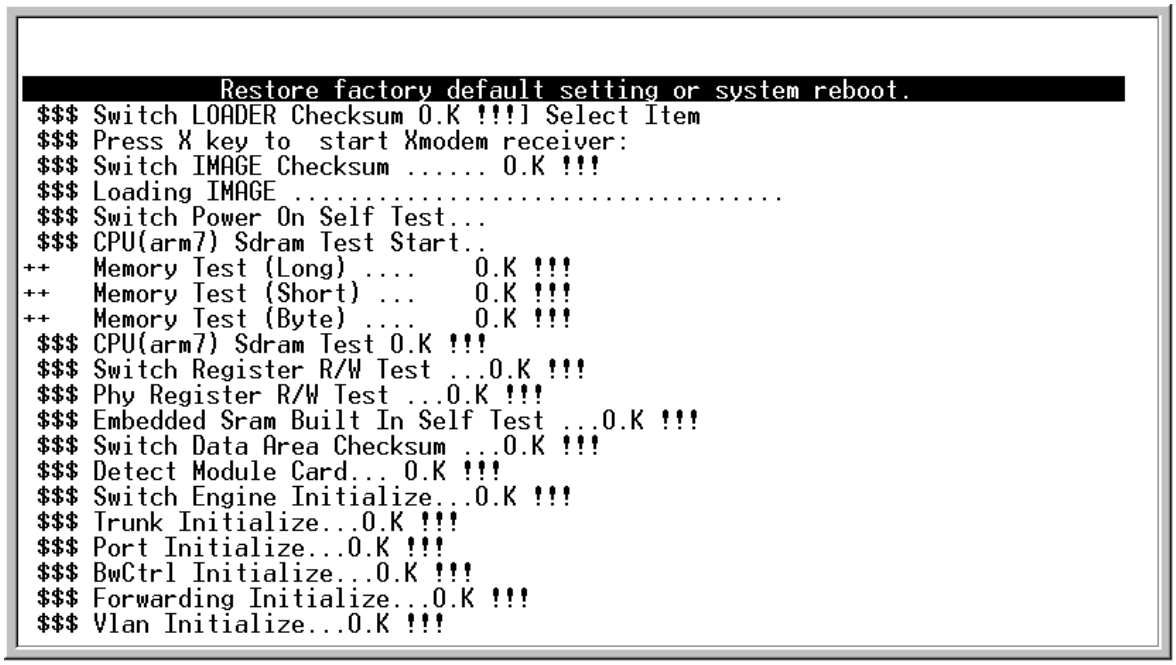
1. Press "**Y**", switch will load default setting.



2. The below figure will tell user that it is restoring to factory default setting.

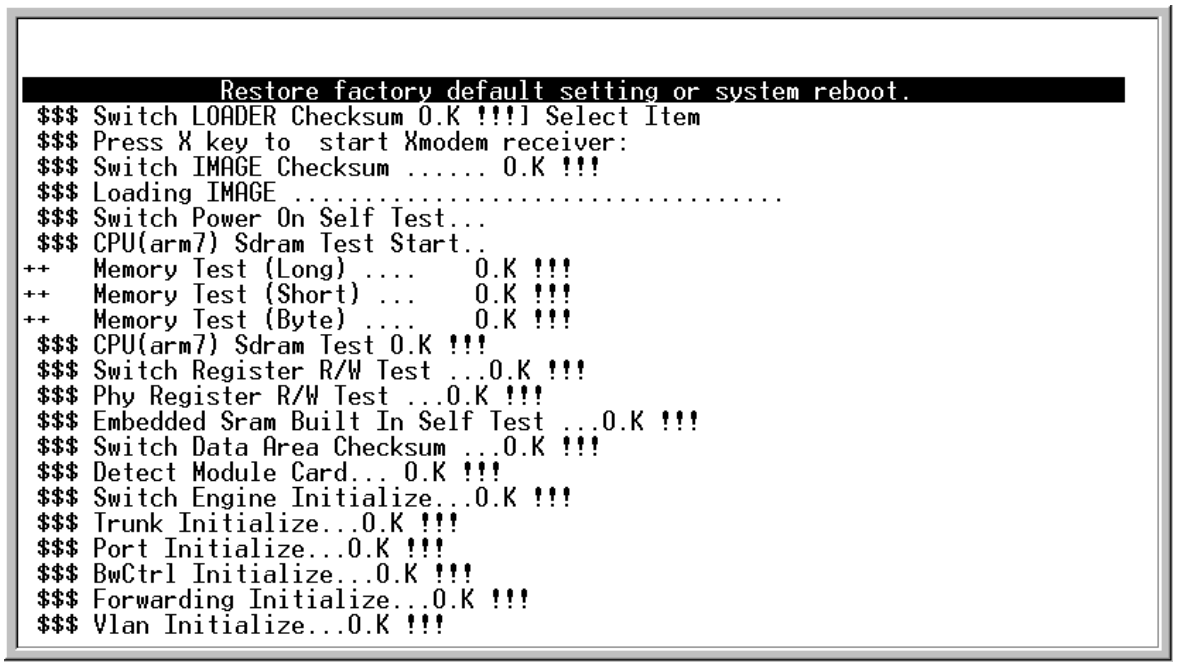


3. After finished load default setting, switch will reboot automatically. The rebooting process will display as below.


Restore factory default setting or system reboot.
$$$ Switch LOADER Checksum O.K !!!] Select Item
$$$ Press X key to start Xmodem receiver:
$$$ Switch IMAGE Checksum ..... O.K !!!
$$$ Loading IMAGE .....
$$$ Switch Power On Self Test...
$$$ CPU(arm7) Sdram Test Start..
++ Memory Test (Long) .... O.K !!!
++ Memory Test (Short) ... O.K !!!
++ Memory Test (Byte) .... O.K !!!
$$$ CPU(arm7) Sdram Test O.K !!!
$$$ Switch Register R/W Test ...O.K !!!
$$$ Phy Register R/W Test ...O.K !!!
$$$ Embedded Sram Built In Self Test ...O.K !!!
$$$ Switch Data Area Checksum ...O.K !!!
$$$ Detect Module Card... O.K !!!
$$$ Switch Engine Initialize...O.K !!!
$$$ Trunk Initialize...O.K !!!
$$$ Port Initialize...O.K !!!
$$$ BwCtrl Initialize...O.K !!!
$$$ Forwarding Initialize...O.K !!!
$$$ Vlan Initialize...O.K !!!

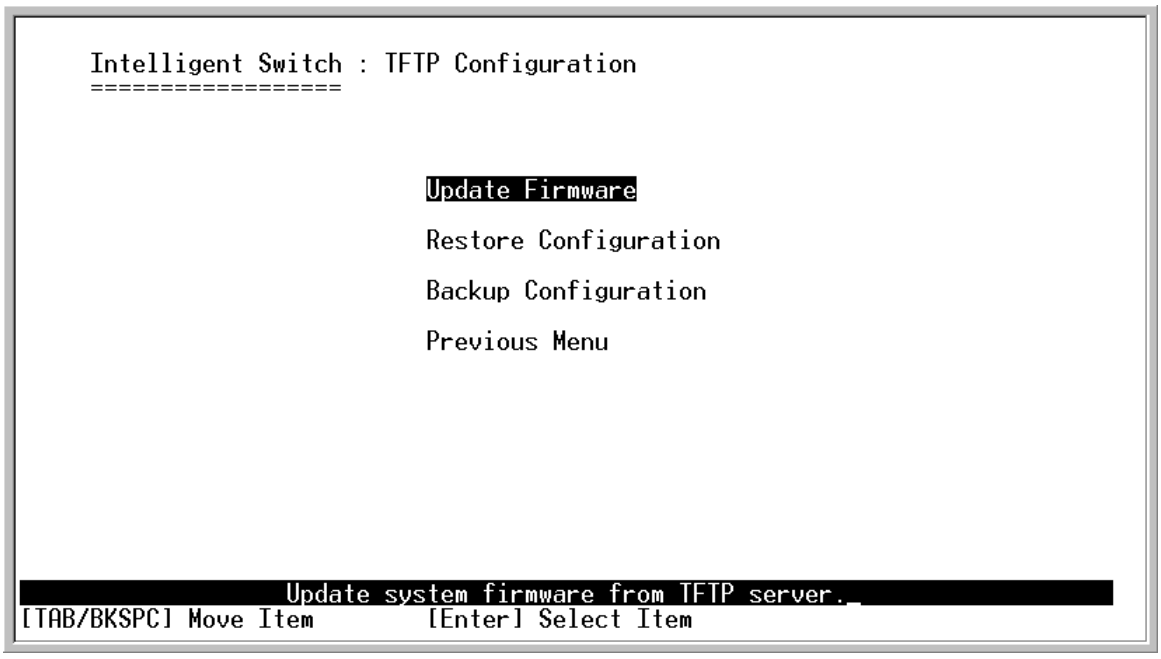
System Reboot

Reboot the switch in software reset. The rebooting process will display as below.


Restore factory default setting or system reboot.
$$$ Switch LOADER Checksum O.K !!!] Select Item
$$$ Press X key to start Xmodem receiver:
$$$ Switch IMAGE Checksum ..... O.K !!!
$$$ Loading IMAGE .....
$$$ Switch Power On Self Test...
$$$ CPU(arm7) Sdram Test Start..
++ Memory Test (Long) .... O.K !!!
++ Memory Test (Short) ... O.K !!!
++ Memory Test (Byte) .... O.K !!!
$$$ CPU(arm7) Sdram Test O.K !!!
$$$ Switch Register R/W Test ...O.K !!!
$$$ Phy Register R/W Test ...O.K !!!
$$$ Embedded Sram Built In Self Test ...O.K !!!
$$$ Switch Data Area Checksum ...O.K !!!
$$$ Detect Module Card... O.K !!!
$$$ Switch Engine Initialize...O.K !!!
$$$ Trunk Initialize...O.K !!!
$$$ Port Initialize...O.K !!!
$$$ BwCtrl Initialize...O.K !!!
$$$ Forwarding Initialize...O.K !!!
$$$ Vlan Initialize...O.K !!!

TFTP Configuration

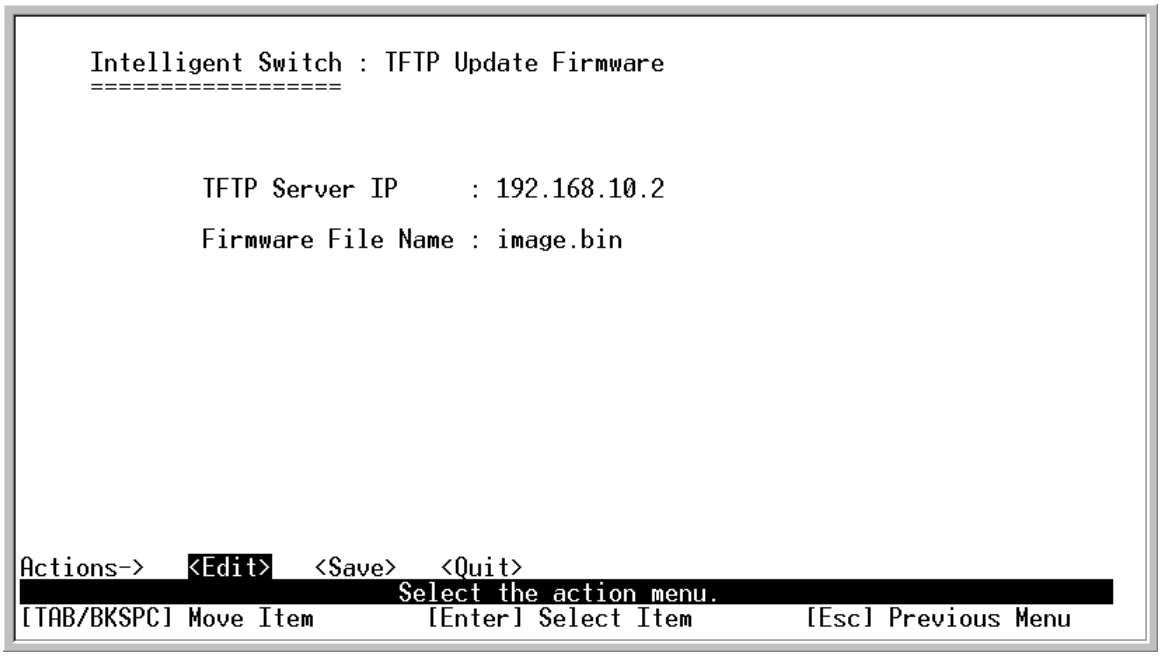
It provides user to update firmware or restore EEPROM value or upload current EEPROM value.



■ Update Firmware

It provides the TFTP updating firmware.

1. Start the TFTP server, and copy new firmware version image file to the TFTP server.
2. Select **<Edit>**.
3. **TFTP Server IP:** type the IP of TFTP server.
4. **Firmware File Name:** type the image file name.
5. Press "**ESC**" to back to action line.
6. Select **<Save>**, the system will start to download the image file.
7. When save successfully, the image file download finished, too.
8. Restart switch.

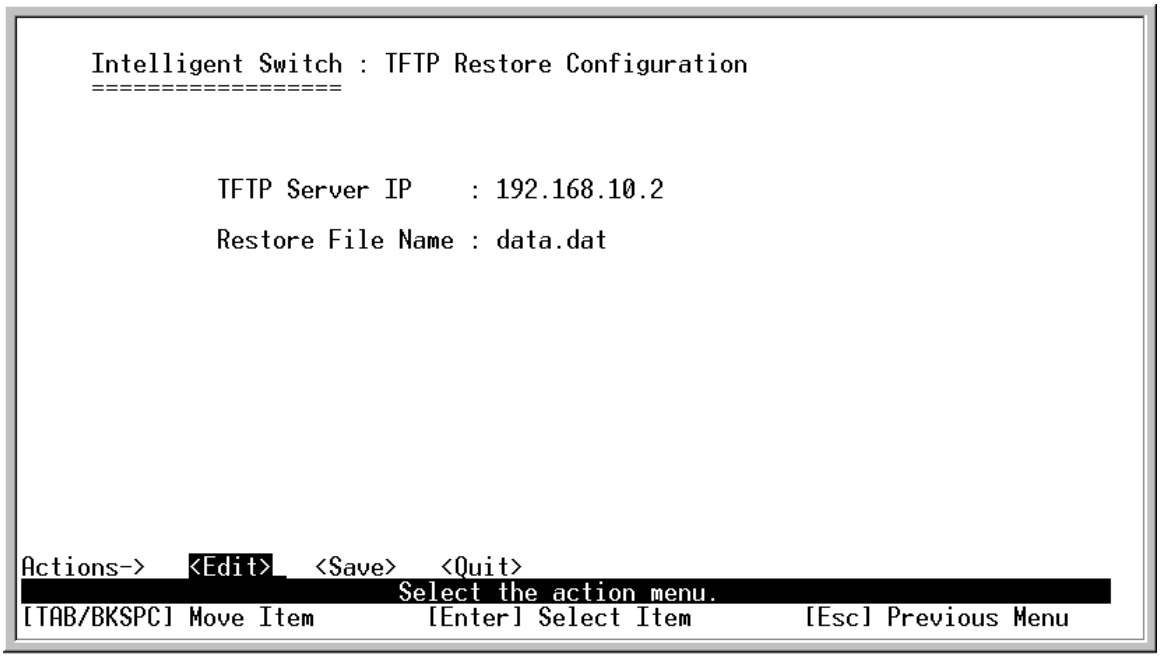

Intelligent Switch : TFTP Update Firmware
TFTP Server IP : 192.168.10.2
Firmware File Name : image.bin
Actions-> <Edit> <Save> <Quit>
Select the action menu.
[TAB/BKSPC] Move Item [Enter] Select Item [Esc] Previous Menu

■ TFTP Restore Configuration

You can restore EEPROM value, which saved in TFTP server, from TFTP server.

1. Start the TFTP server.
2. Select **<Edit>**.
3. **TFTP Server IP:** type the IP of TFTP server.
4. **Restore File Name:** type the image file name.

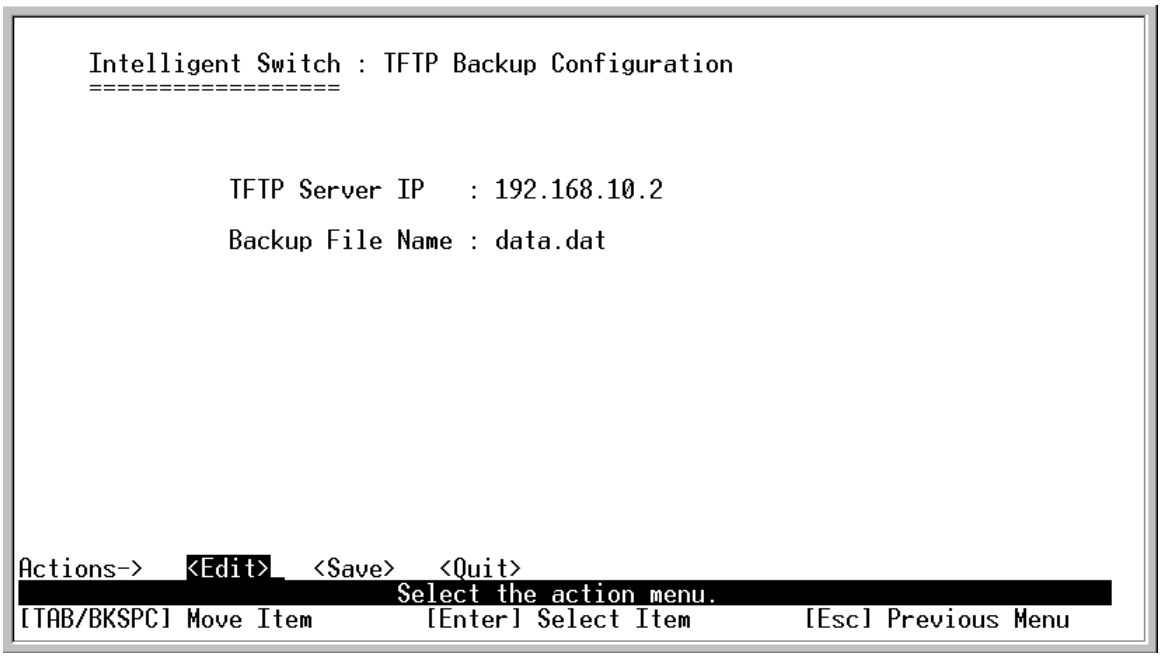
5. Press “**ESC**” back to action menu line.
6. Select **<Save>**, it will start to download the image file.
7. When save successfully, the image file download finished too.
8. Restart switch.


Intelligent Switch : TFTP Restore Configuration
TFTP Server IP : 192.168.10.2
Restore File Name : data.dat
Actions-> <Edit> <Save> <Quit>
Select the action menu.
[TAB/BKSPC] Move Item [Enter] Select Item [Esc] Previous Menu

■ TFTP Backup Configuration

You can save current EEPROM value to TFTP server as backup. The backup file can be restored from TFTP server when you need.

1. Start the TFTP server.
2. Select **<Edit>**.
3. **TFTP Server IP:** type the IP of TFTP server.
4. **Backup File Name:** type the image file name.
5. Press “**ESC**” back to action line.
6. Select **<Save>** key, it will start to upload the image file.
7. When save successfully, the image file upload finished too.
8. Restart switch.


Intelligent Switch : TFTP Backup Configuration
TFTP Server IP : 192.168.10.2
Backup File Name : data.dat
Actions-> <Edit> <Save> <Quit>
Select the action menu.
[TAB/BKSPC] Move Item [Enter] Select Item [Esc] Previous Menu

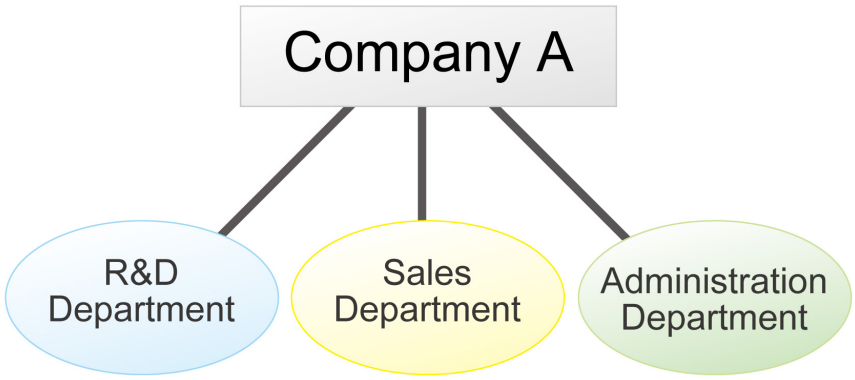
6 Application Example: VLAN Network

In this chapter, you will learn how to deploy VLAN network in office. VLAN is a simple and useful solution to protect your network against broadcast storming by creating segments based on Layer 2 Ethernet information. Besides, it offers security by completely isolating from each other.

6.1 Application Environment

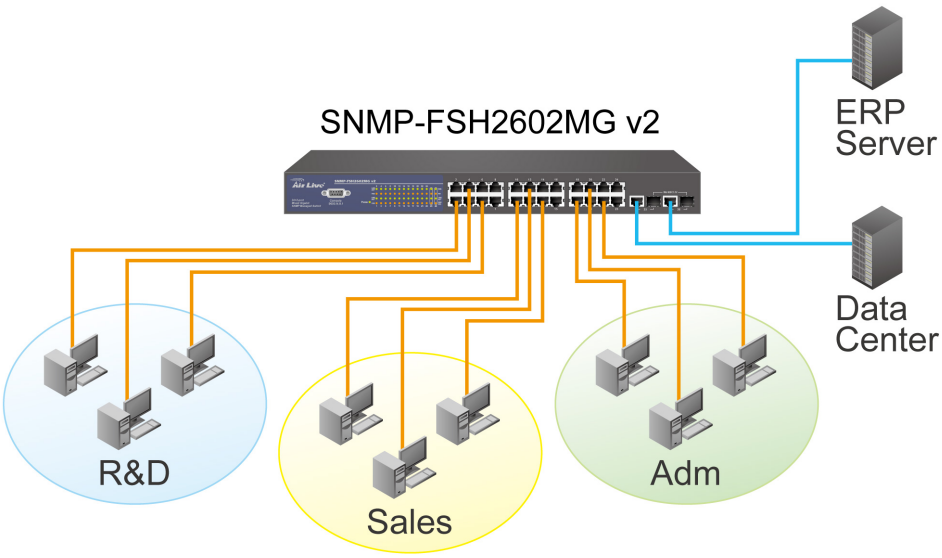
There are some departments in a business company, such as Sales department, R&D department. These departments can share the same company resource, such as ERP system, print server. Here is one simple example for users to use VLAN function well.

The organization structure of Company A is below:



Company A has tree main departments, **Sales department, R&D department, and Administration department**. Members in different departments can share the same network resource, such as ERP server and data center. Besides, for need of department information privacy, members with departments cannot communicate with each other.

For fulfilling above requirement, the network topology of Company A could be below:



6.2 VLAN Configuration

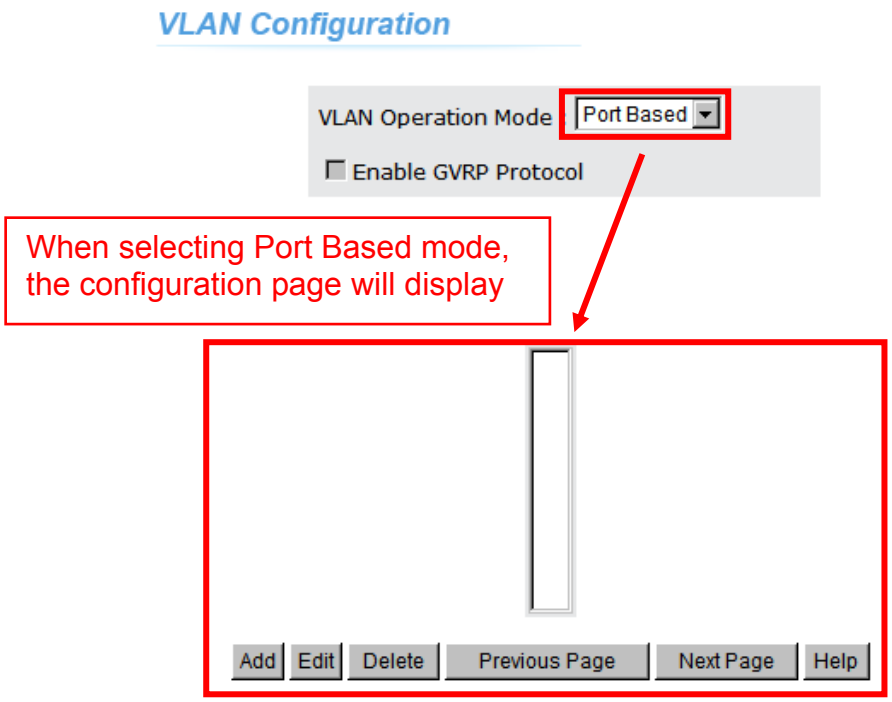
There are two ways to deploy above network topology in VLAN configuration. They are Port Based VLAN and 802.1Q VLAN (Tag VLAN), respectively. User can refer to the following configuration in detail.

The **basic consumption** is below

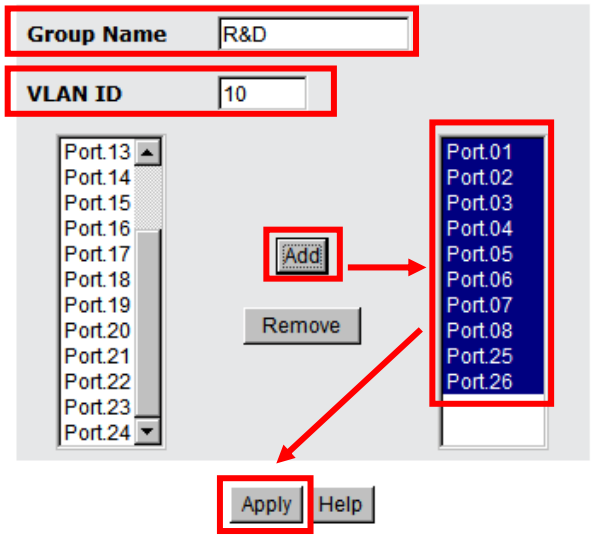
- ERP server, data center or some shared servers are connected to port 25 and port 26, respectively
- R&D department can use port 1 to port 8; Sales department can use port 9 to port 16; Administration department can use port 17 to port 24.
- Departments cannot communicate each other, but can access ERP server and data center.

6.2.1 Configuration of Port Based VLAN

Step 1 Select VLAN operation mode to **Port Based**, then the configuration page will display.



Step 2 Click "**Add**" button to create one VLAN group whose group name is "R&D", VLAN is 10, member ports are port 1 to port 8, port 25, and port 26. Click "**Apply**" button to create your VLAN group.



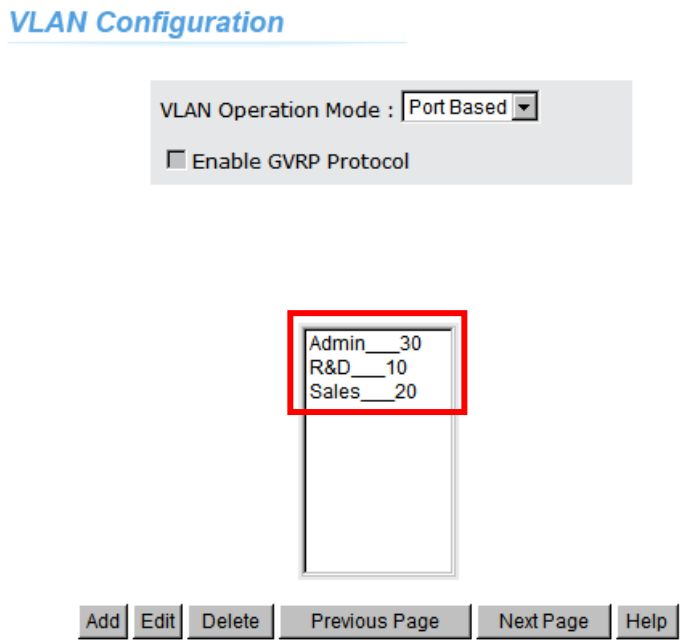
Step 3 Follow Step 2 to create another two VLAN groups.

The detailed setting is below:

- Group name: R&D, VLAN ID: 10, member ports: port 1 to 8; port 25, port 26
- Group name: Sales, VLAN ID: 20, member ports: port 9 to 16; port 25, port 26
- Group name: Admin, VLAN ID: 30, member ports: port 17 to 24; port 25, port

26.

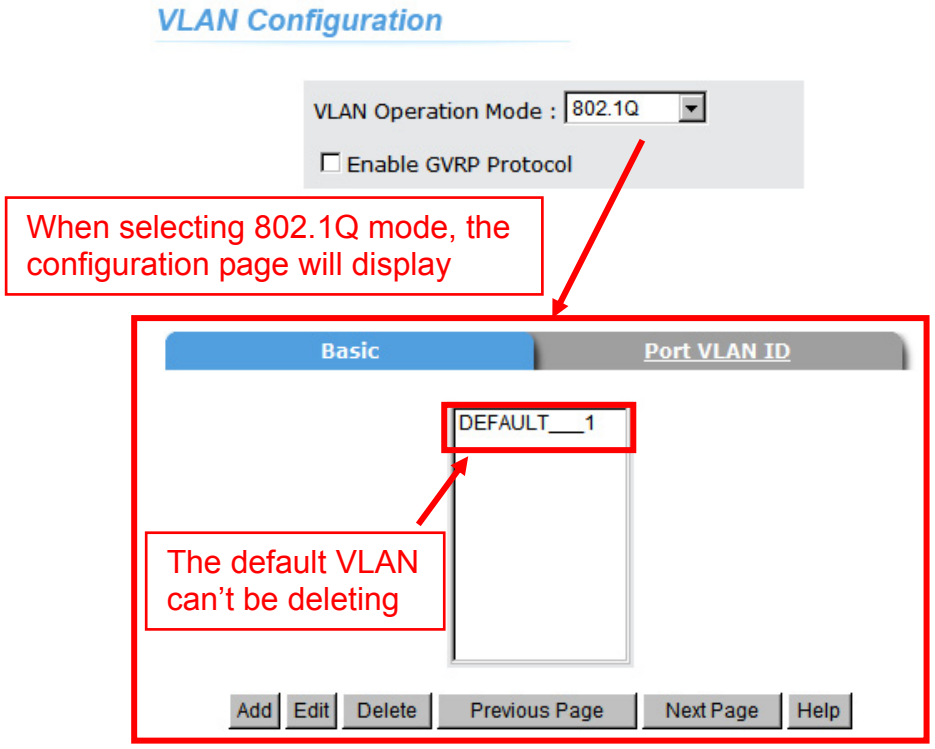
The result of VLAN configuration will display as below:



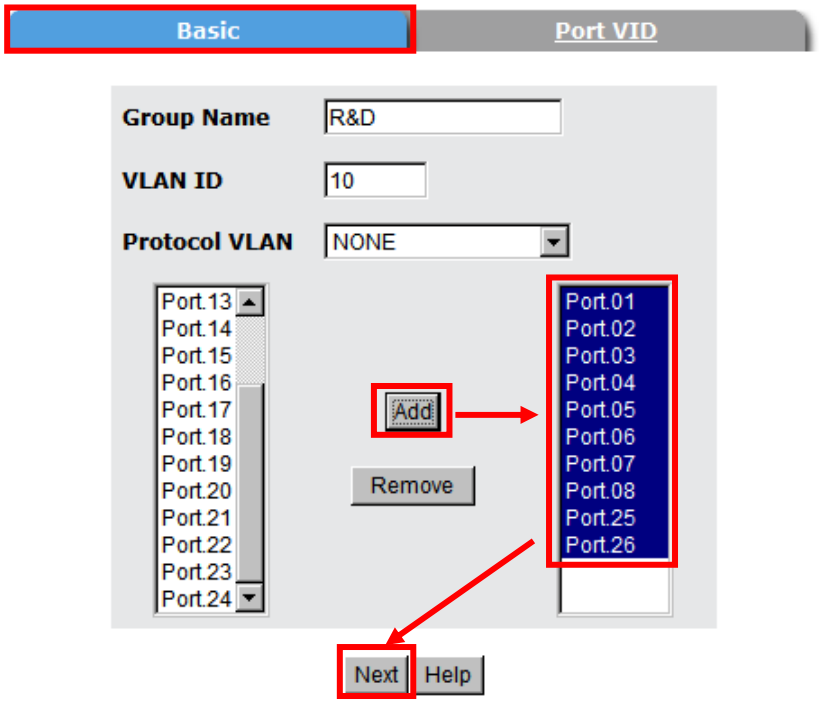
After finishing above steps, the Tag VLAN function can work as your need.

6.2.2 Configuration of 802.1Q VLAN

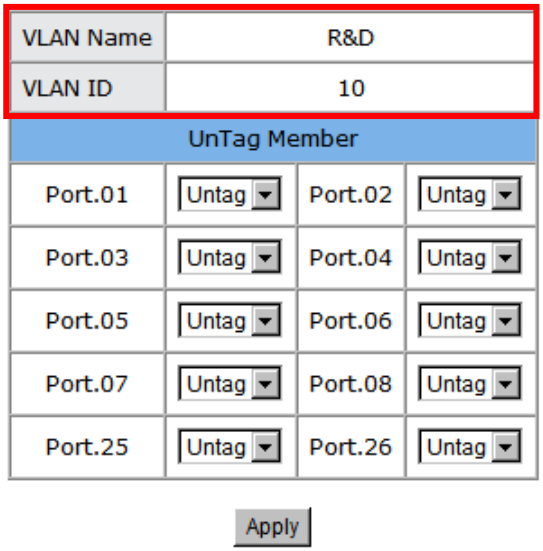
Step 1 Select VLAN operation mode to **802.1Q**, then the configuration page will display.



Step 2 Click "**Add**" button to create one VLAN group whose group name is "R&D", VLAN is 10, member ports are port 1 to port 8, port 25, and port 26. Click "**Next**" button to configure other settings.



Step 3 While clicking "**Next**" button, user does need to any change on this page.

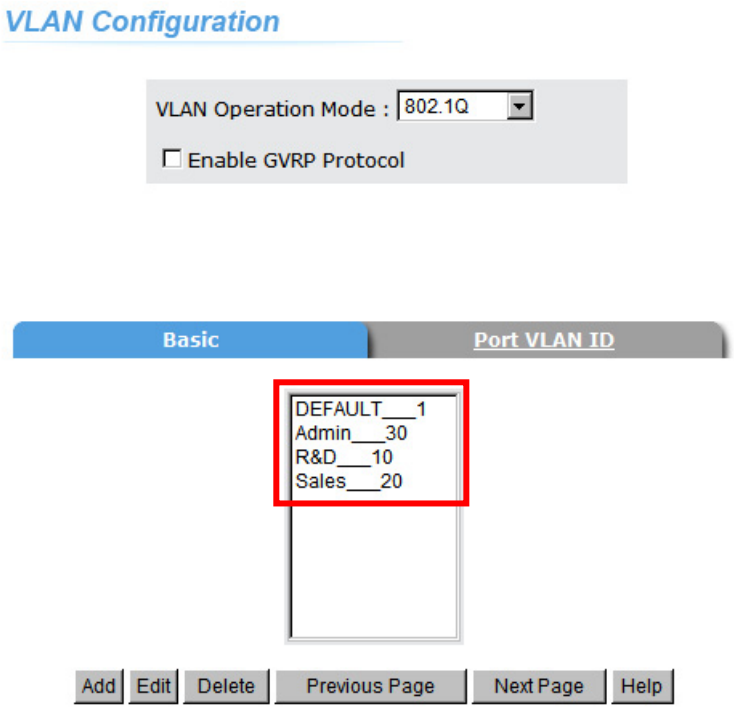


Step 4 Follow Step 2 and Step 3 to create another three VLAN group.

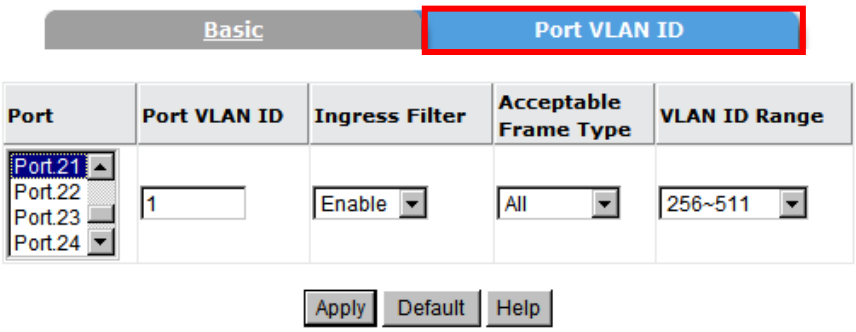
The detailed setting is below:

- Group name: R&D, VLAN ID: 10, member ports: port 1 to 8; port 25, port 26
- Group name: Sales, VLAN ID: 20, member ports: port 9 to 16; port 25, port 26
- Group name: Admin, VLAN ID: 30, member ports: port 17 to 24; port 25, port 26.

The result of VLAN configuration will display as below:

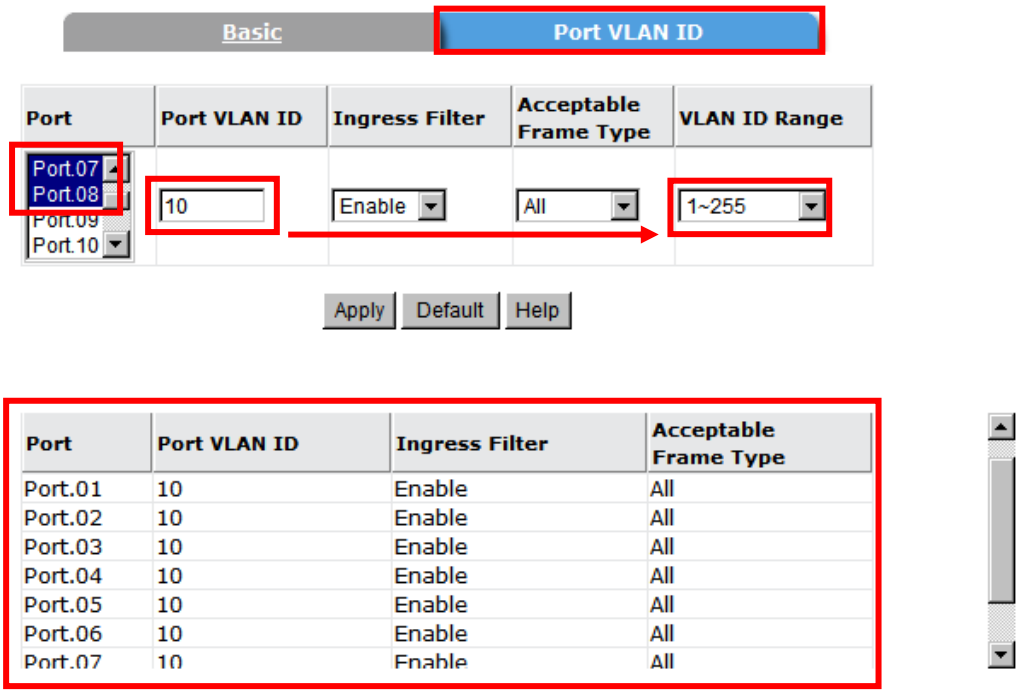


Step 5 Click “Port VLAN ID” page to configure PVID setting.



Port	Port VLAN ID	Ingress Filter	Acceptable Frame Type
Port.21	1	Enable	All

Step 6 Choose port 1 to port 8 in port menu, enter Port VLAN ID as 10, and select VLAN ID Range to 1~255. Then, click “**Apply**” button to apply your setting.



Port	Port VLAN ID	Ingress Filter	Acceptable Frame Type
Port.01	10	Enable	All
Port.02	10	Enable	All
Port.03	10	Enable	All
Port.04	10	Enable	All
Port.05	10	Enable	All
Port.06	10	Enable	All
Port.07	10	Enable	All

Step 6 Follow Step 6, the detailed setting is below:

- Port 1 to 8: Port VLAN ID is 10, VLAN ID Range is 1~255
- Port 9 to 16: Port VLAN ID is 20, VLAN ID Range is 1~255
- Port 17 to 24: Port VLAN ID is 30, VLAN ID Range is 1~255

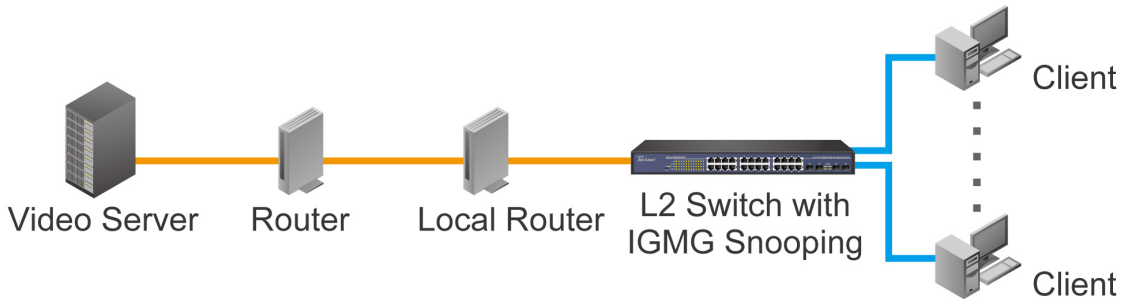
After finishing above steps, the Tag VLAN function can work as your need.

7 Application Example: IGMP Snooping

In this section, we will build IP Multicast network environment, and explain how IGMP Snooping works in SNMP-FSH2602MG v2. Having this application example, user can easily know advantage of IGMP Snooping.

7.1 Application Environment

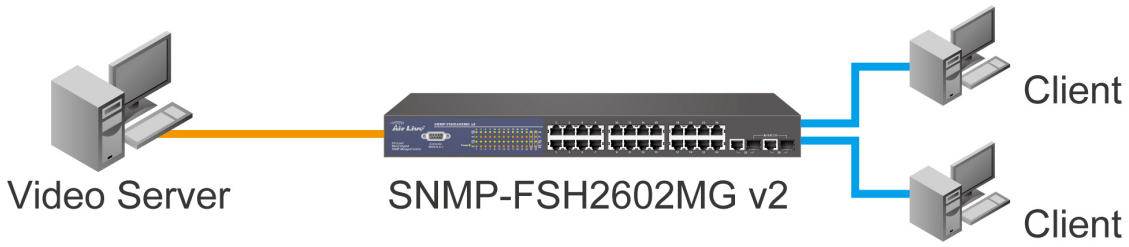
A network designed to deliver a multicast service (like video) using IGMP might use this basic network structure:



For easily understanding how IGMP Snooping works in SNMP-FSH2602MG v2, we simplify the above structure. We use one PC as video server, two PCs as video clients; SNMP-FSH2602MG v2 connects them, and use VLC media player (version 0.8.1) as

media software.

Video server whose IP address (group) is 239.1.1.1 connects to port 9 of SNMP-FSH2602MG v2 via RJ-45 cable, and video client connects to port 13 of SNMP-FSH2602MG v2 via RJ-45 cable.

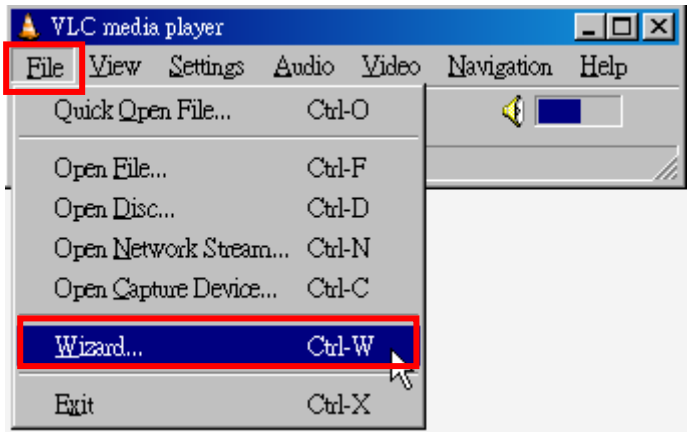


7.2 Configuration of video server and client

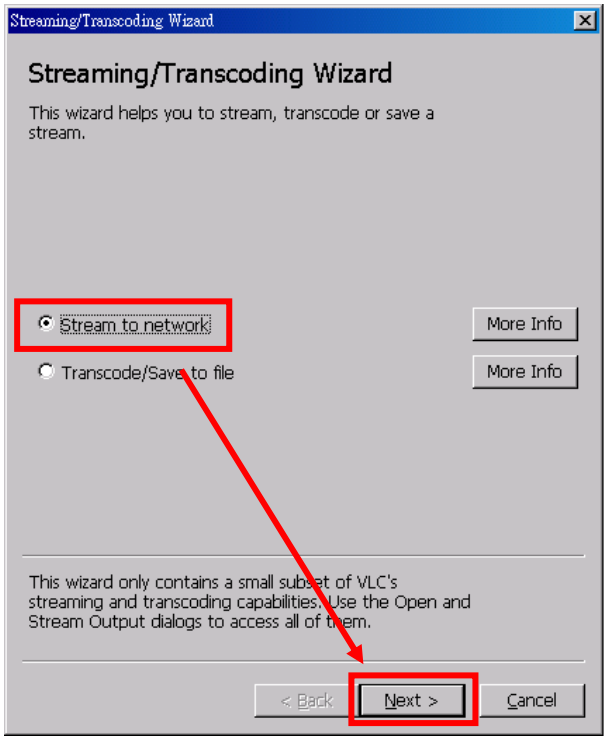
Before following the above steps, please install VLC media server in advance. Please refer to www.vidoelan.org for better knowing.

7.2.1 Video Server

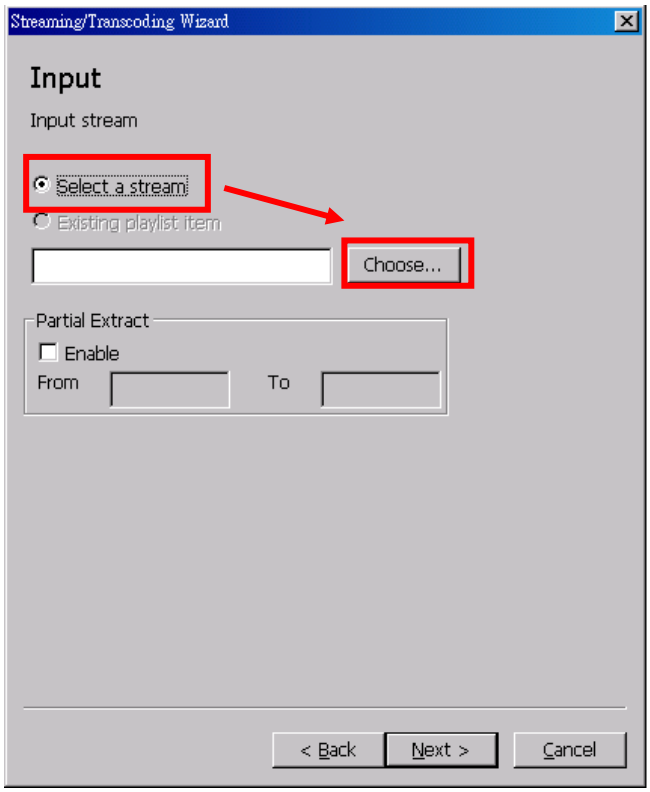
Step 1 Execute VLC, and click "**File**"> "**Wizard**"



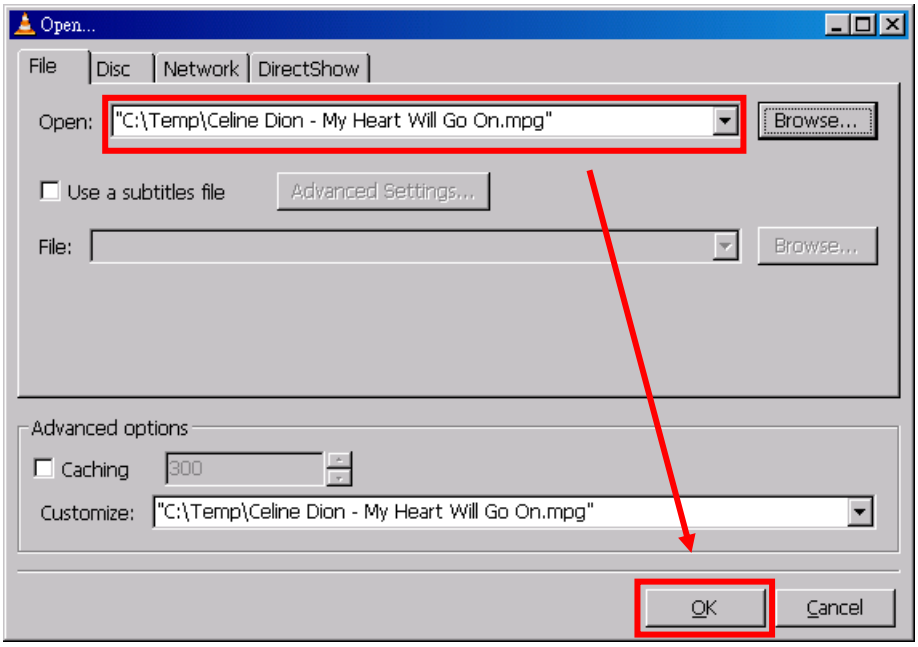
Step 2 Check "**Stream to network**", and then click "**Next**".


Streaming/Transcoding Wizard
Streaming/Transcoding Wizard
This wizard helps you to stream, transcode or save a stream.
Stream to network
Transcode/Save to file
More Info
More Info
This wizard only contains a small subset of VLC's streaming and transcoding capabilities. Use the Open and Stream Output dialogs to access all of them.
< Back
Next >
Cancel

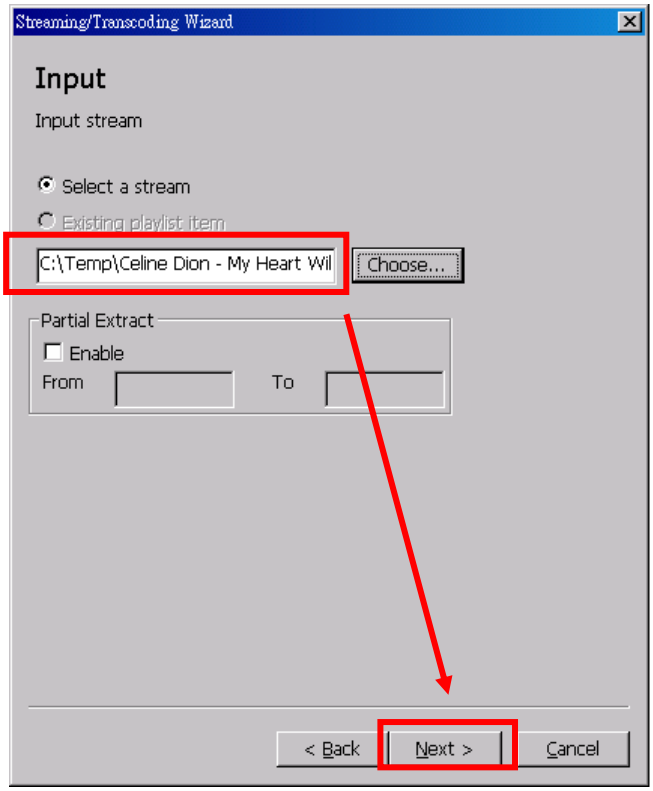
Step 3 Check "**Select a stream**", and then click "**Choose**" to choose your media files which will be played.



Step 4 In this page, choose one media file, and then click "**OK**" button.

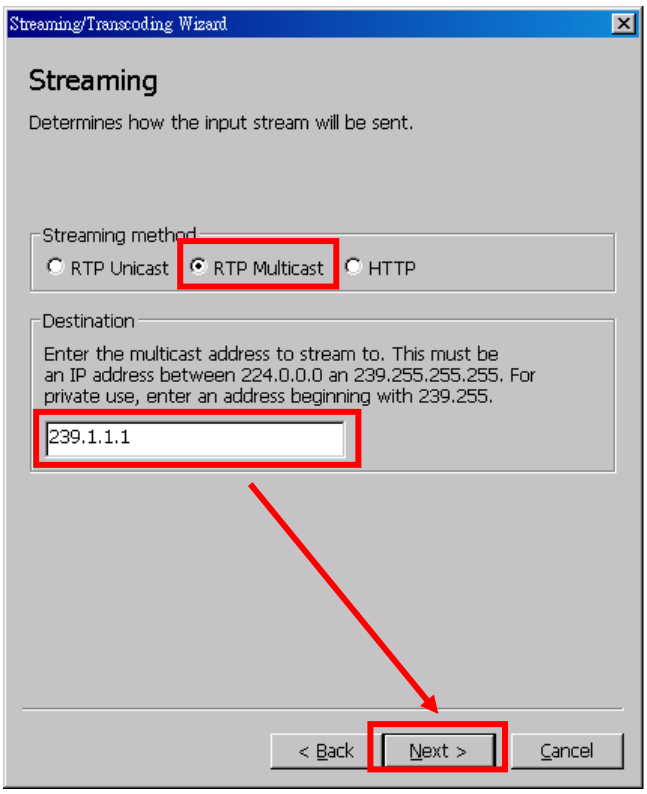


Step 5 After entering directory of media file, and then click "**Next**" to do next step.

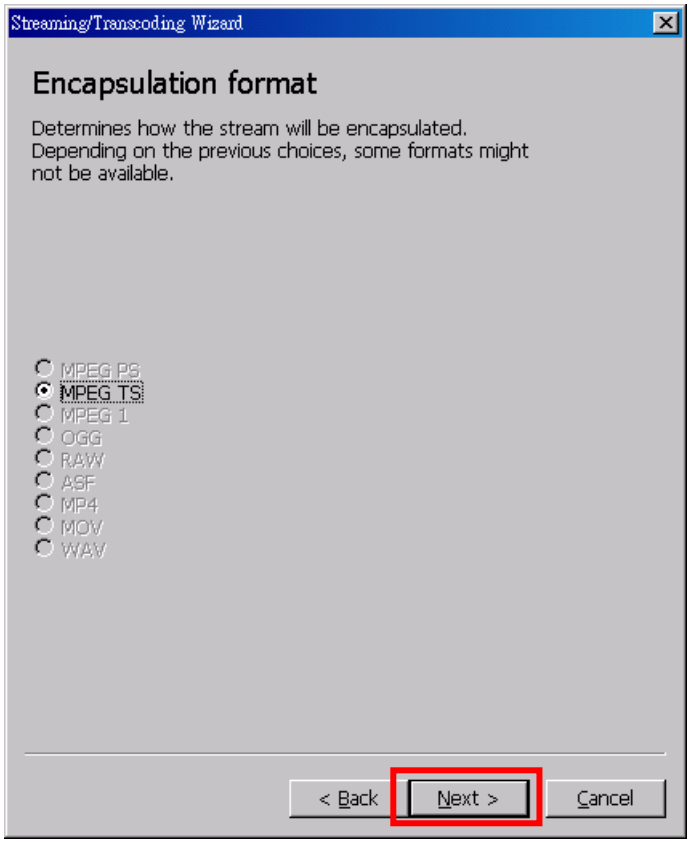


Step 6 Check "**RTP Multicast**" to enter multicast address of video server, and then click "**Next**" to do next step.

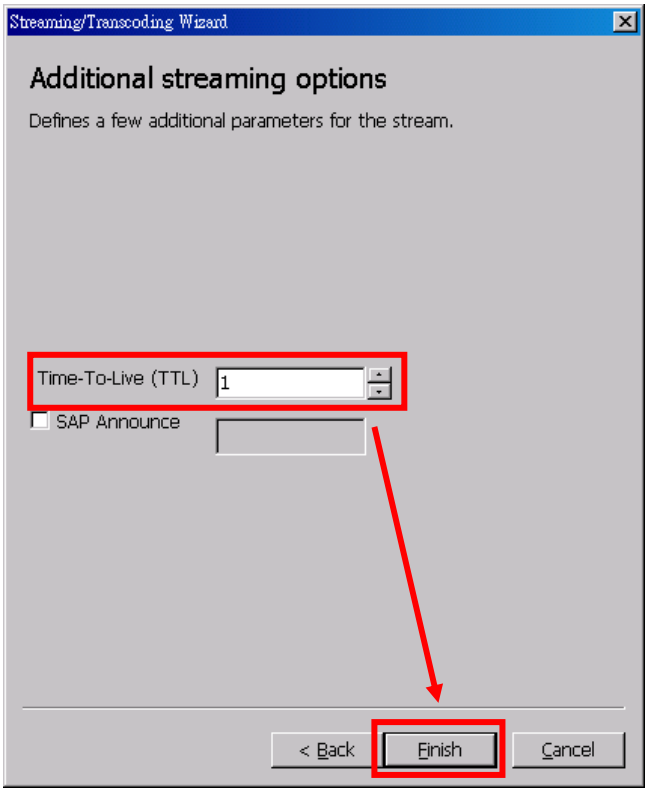
Note: IP range of multicast address must be between 224.0.0.0 and 239.255.255.255.


Streaming/Transcoding Wizard
Streaming
Determines how the input stream will be sent.
Streaming method
RTP Unicast
RTP Multicast
HTTP
Destination
Enter the multicast address to stream to. This must be an IP address between 224.0.0.0 an 239.255.255.255. For private use, enter an address beginning with 239.255.
239.1.1.1
< Back
Next >
Cancel

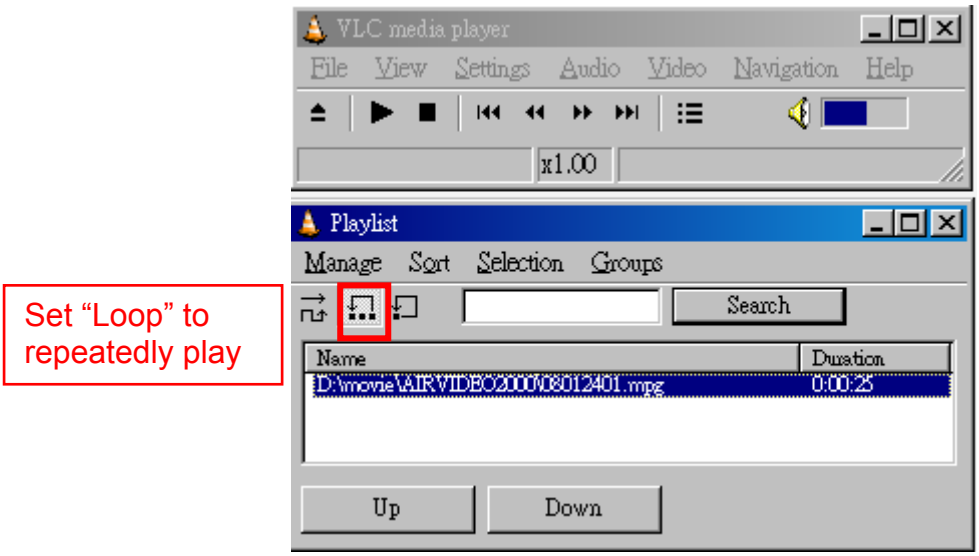
Step 7 Check **encapsulation format** as you want, and then click "**Next**" to do next step.



Step 8 Enter TTL as your need, and then click "**Finish**" to finish configuration of video server.



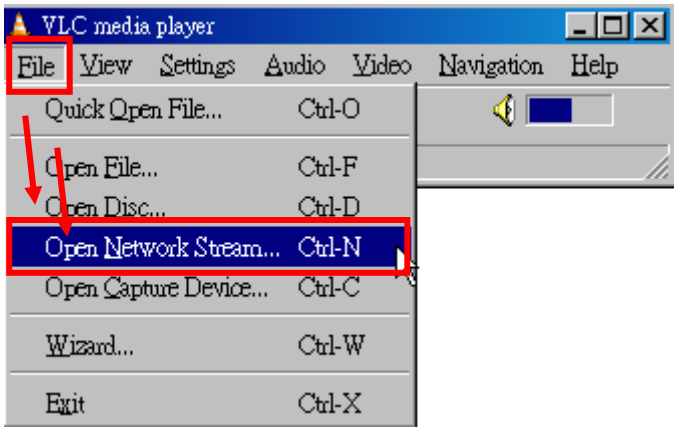
Step 9 Select "**View**"> "**Playlist**" and set "Loop" to repeatedly play.



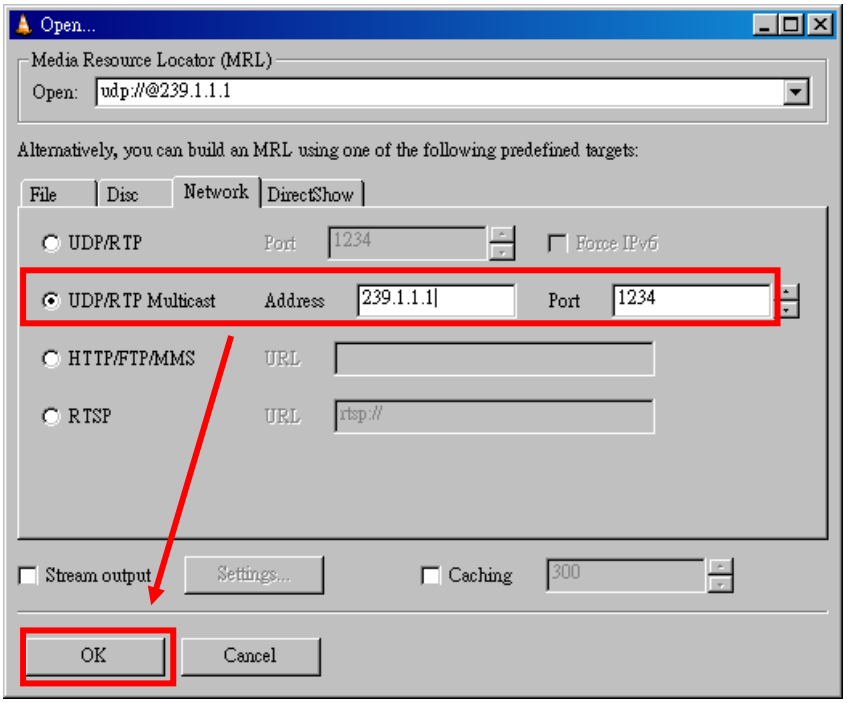
7.2.2 Video client

Video clients are interested in content of group 239.1.1.1, so they can join group 239.1.1.1 via multicast to view the video..

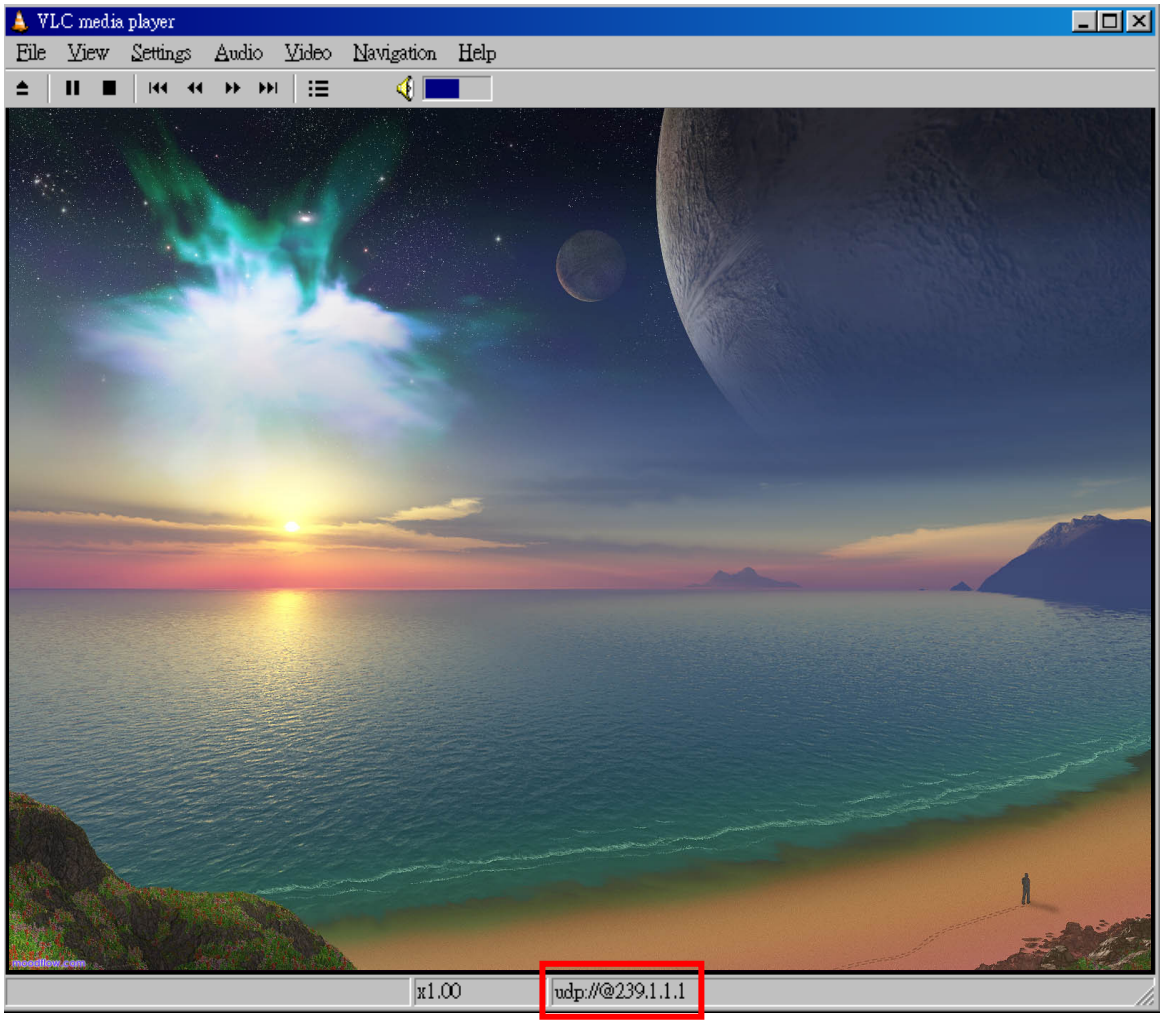
Step 1 Execute VLC, and click "**File**"> "**Wizard**"



Step 2 Check "**UDP/RTP Multicast**", and enter IP address and port number of video server. Then, click "**OK**" to finish configuration of video client.



Step 3 VLC media player will play multimedia file from 239.1.1.1 (IP address of video server).

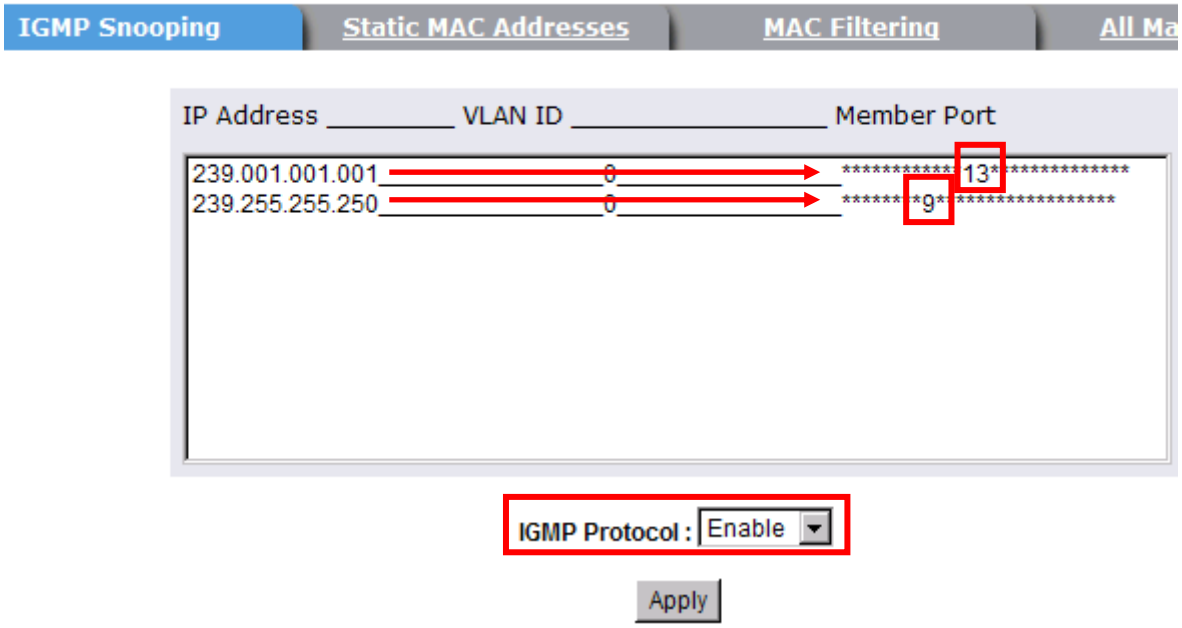


7.3 IGMP Snooping in SNMP-FSH2602MG v2

When enabling function of IGMP Snooping, SNMP-FSH2602MG v2 will listen in on IGMP traffic. Please click "**Administrator**" > "**Forwarding and Filtering**" > "**IGMP Snooping**".

From WebUI, user can know that video client (port 13) joins "multicast group 239.1.1.1", and there is one multicast group connecting port 9. With snooping function, Switch can easily know that when receiving packets from multicast group 239.1.1.1, it just only transmits packets to port 13, does not need transmit packets to other ports, it will reduce switch loading.

Forwarding and Filtering



8 Troubleshooting

This section is intended to help you solve the most common problems on the SNMP-FSH2602MG v2.

8.1 Incorrect connections

The switch port can auto detect straight or crossover cable when you link switch with other Ethernet device. For the RJ-45 connector should use correct UTP or STP cable, 10/100Mbps port use 2 pairs twisted cable and Gigabit 1000T port use 4 pairs twisted cable. If the RJ-45 connector is not correct pin on right position then the link will fail. For fiber connection, please notice that fiber cable mode and fiber module should be match.

■ Faulty or loose cables

Look for loose or obviously faulty connections. If they appear to be OK, make sure the connections are snug. IF that does not correct the problem, try a different cable.

■ Non-standard cables

Non-standard and miss-wired cables may cause numerous network collisions and other network problem, and can seriously impair network performance. A category 5-cable tester is a recommended tool for every 100Base-T network installation.

■ Improper Network Topologies

It is important to make sure that you have a valid network topology. Common topology faults include excessive cable length and too many repeaters (hubs) between end nodes. In addition, you should make sure that your network topology contains no data path loops. Between any two ends nodes, there should be only one active cabling path at any time. Data path loops will cause broadcast storms that will severely impact your network performance.

8.2 Diagnosing LED Indicators

The SNMP-FSH2602MG v2 can be easily monitored through panel indicators to assist in identifying problems, which describes common problems you may encounter and where you can find possible solutions. Please refer to Chapter 2.2 for detailed information.

If the power indicator does turn on when the power cord is plugged in, you may have a problem with power outlet, or power cord. However, if the Switch powers off after running for a while check for loose power connections, power losses or surges at power outlet. IF you still cannot resolve the problem, contact your local dealer for assistance.

8.3 Cabling

RJ-45 ports: use unshielded twisted-pair (UTP) or shield twisted-pair (STP) cable for RJ-45 connections: 100Ω Category 3, 4 or 5 cable for 10Mbps connections or 100Ω Category 5 cable for 100Mbps connections. Also be sure that the length of any twisted-pair connection does not exceed 100 meters (328 feet). Gigabit port should use Cat-5 or cat-5e cable for 1000Mbps connections. The length does not exceed 100 meters.

9 Specifications

This section provides the specifications of SNMP-FSH2602MG v2, and the following table lists these specifications.

Standard	● IEEE802.3 10BASE-T ● IEEE802.3u 100BASE-TX/100BASE-FX ● IEEE802.3z Gigabit SX/LX ● IEEE802.3ab Gigabit 1000T ● IEEE802.3x Flow Control and Back pressure ● IEEE802.3ad Port trunk with LACP ● IEEE802.1d Spanning tree protocol ● IEEE802.1p Class of service ● IEEE802.1Q VLAN Tagging ● IEEE802.1w Rapid Spanning tree protocol
Interface	● 24 x 10/100Mbps Auto-negotiation, Auto-MDIX ports ● 2 x 1000Base-T/mini GBIC ports (combo)
Switch architecture	● Store and forward switch architecture. ● Back-plane up to 8.8Gbps
MAC address	● 8K
Memory	● 3Mbits for packet buffer
Flash ROM	● 512Kbytes

System memory	● 8Mbytes
LED	● System power ● 10/100Base-TX: Link/Activity, Full Duplex/Collision ● 1000Base-T: 100, 1000, Link/Activity, Full Duplex/Collision
Management	● Telnet/ Web/ SNMP v1 management, RS-232 console management ● RFC Standard ■ RFC 1157 SNMP, RFC 1213 MIB II, RFC 1643 Ethernet like, RFC 1493 Bridge MIB, RFC 1757 RMON 1, RFC 1215 Trap, RFC 2674 VLAN MIB, private MIB ● SNMP Trap ■ Cold start, link down, link up, authorization fail. ■ Trap station up to 3. ● TFTP and Console firmware upgradeable ● Port Trunk ■ Support IEEE802.3ad with LACP function. ■ Up to 7 trunk groups and group member up to 4. ■ Trunk port within 24-port 10/100TX and 2 Ext. Gigabit port ● Supports IEEE802.1d STP & IEEE802.1w RSTP ● VLAN ■ Port based VLAN ■ IEEE802.1Q Tag VLAN ■ GVRP ■ IEEE802.1v Protocol VLAN (IP, IPX,..) ■ Static VLAN groups up to 256, Dynamic VLAN group up to 2048, VLAN ID from 0 to 4094 ● QoS policy: Supports 8 priority levels ID for two priority queue ● Class of Service

	■ High and low queues. ■ Priority service rule: first come first service, all High before Low, WRR for High or low weight. ● Supports Port-based Priority ● Supports IGMP V1 and V2 snooping ● Supports IP stacking, up to 8 units ● Supports ingress and egress MAC address filter and static source MAC address lock ● Supports Port Mirroring ● Supports Broadcast Storm Control ● Supports Bandwidth Control, per level 100Kbps ● Supports 802.1x Authentication ■ Reject ■ Accept ■ Authorize ■ Disable ● Support DHCP client ● Supports Broadcast storm filter
MTBF	● 39797.78863 (hr)
Temperature	● Operating: 0 to 40°C ● Storage: -10 to 70°C
Humidity	● Operating: 10% ~ 90% ● Storage: 5% ~ 90%
Power	● 100~240VAC 50/60Hz, 0.8 A (maximum) ● Power consumption 34 Watts
Produce Weight (g)	● 2150 g

Dimensions	● 440 x 161 x 44 mm

10 Network Glossary

The network glossary contains explanation or information about common terms used in wireless networking products. Some of information in this glossary might be outdated, please use with caution.

100Base-FX

The IEEE standard defines how to transmit Fast Ethernet 100Mbps data using multi-mode or single fiber optic cable

100Base-TX

Also known as 802.3u. The IEEE standard defines how to transmit Fast Ethernet 100Mbps using Cat.5 UTP/STP cable. The 100Base-TX standard is backward compatible with the 10Mbps 10-BaseT standard.

1000Base-SX

Also known as 802.3z. The IEEE standard defines how to transmit gigabit Ethernet data using multi-mode fiber optic cables. This standard allows transmission distance of 550 meter, which is more than 5 times longer than the 100-meter limitation of 1000Base-T. The 1000Base-SX cannot run in 100Mbps mode.

1000Base-LX

The IEEE standard defines how to transmit gigabit Ethernet data using single mode fiber optic cables. This standard allows transmission distance of 5km or more using single mode fiber. The 1000Base-LX cannot run in 100Mbps mode.

1000Base-T

Also known 802.3ab standard. The IEEE standard defines how to transmit Gigabit data through the use of Cat.5 UTP/STP cable. The 1000Base-T can run in 10/100/1000Mbps

speed, and is backward compatible with 10/100Base-TX standard.

802.1d STP

Spanning Tree Protocol. It is an algorithm to prevent network from loop topology. Spanning tree allows a network design to include spare (redundant) links to provide automatic backup paths if an active link fails, without the danger of bridge loops, or the need for manual enabling/disabling of these backup links. Bridge loop must be avoided because of flooding issue in the network.

802.1Q Tag VLAN

In 802.1Q VLAN, the VLAN information is written into the Ethernet packet itself. Each packet carries a VLAN ID(called Tag) as it traveled across the network. Therefore, the VLAN configuration can be configured across multiple switches. In 802.1Q spec, possible 4096 VLAN ID can be created. Although for some devices, they can only view in frames of 256 ID at a time.

802.1x

802.1x is a security standard for wired and wireless LANs. In the 802.1x parlance, there are usually supplicants (client), authenticator (switch or AP), and authentication server (radius server) in the network. When a supplicants request a service, the authenticator will pass the request and wait for the authentication server to grant access and register accounting. The 802.1x is the most widely used method of authentication by WISP.

802.1w

Rapid Spanning Tree Protocol. It is a refinement of STP, which provides faster spanning tree convergence after a topology change. While STP can take 30 or 50 seconds to respond to a topology change, RSTP is typically able to respond to changes within a second.

DHCP

Dynamic Hosting Configuration Protocol. A protocol that enables a server to dynamically assign IP addresses. When DHCP is used, whenever a computer logs onto the network, it automatically gets an IP address assigned by DHCP server. A DHCP server can either be a designed PC on the network or another network device, such as a router.

Firmware

The program that runs inside embedded device such as AP or Switch. Many network devices are firmware upgradeable through web interface or utility program.

FTP

File Transfer Protocol. A standard protocol for sending files between computer over a TCP/IP network and the internet.

IGMP Snooping

Internet Group Management Protocol. It is a Layer 3 protocol to report IP multicast memberships to neighboring multicast switches and routers. IGMP Snooping is a feature that allows an Ethernet Switch to “listen in” on the IGMP conversation between hosts and routers. When IGMP snooping is enabled in a switch, it prevent hosts on a local network from receiving traffic for a multicast group they have not explicitly joined. It provides switches with a mechanism to prune multicast traffic from links that do not contain a multicast listener (IGMP client).

IP Address

IP (Internet Protocol) is a Layer 3 network protocol that is the basis of all Internet communication. An IP address is 32-bit number that identifies each sender or receiver of information that is sent across the Internet. An IP address has two parts: an identifier of a particular network on the Internet and an identifier of the particular device (which can be a server or a workstation) within that network. The new IPv6 specification supports 128-bit IP address format.

LACP (802.3ad) Trunking

Link Aggregation Control Protocol. It is protocol defines how to combine the several Ethernet ports into one high-bandwidth port to increase the transmission speed. It is also known as port trunking. Both devices must set the trunking feature to work.

MAC

Media Access Control. MAC address provides Layer-2 identification for network devices. Each Ethernet device has its own unique address. The first 6 digits are unique for each device manufacturers. When a network device has MAC access control feature, only the devices with the approved MAC address can connect with the network.

Mbps

Megabits Per Second. One million bits per second; a unit of measurement for data transmission.

MiniGBIC

A type of Gigabit Ethernet module interface that uses SFP (Small Form-factor Pluggable) transceiver. The MiniGBIC equipped with Switches typically comes with the MiniGBIC slot for optional SFP optical transceiver.

Packet

A unit of data sent over a network.

Rate Control

It is an Ethernet switch's function to control the upstream and downstream speed of an individual port. Rate control management use "Flow Control" to limit the speed of a port. Therefore, the Ethernet adapter must also have the flow control enabled. One way to force the adapter's flow control on is to set a port to half-duplex mode.

SNMP

Simple Network Management Protocol. A set of protocols for managing complex networks. The SNMP network contains three key elements: managed devices, agents, and network-management system (NMS). Managed devices are network devices that contain SNMP agents. SNMP agents are programs that reside SNMP capable device's firmware to provide SNMP configuration service. The NMS typically is PC-based software that can monitor and control managed devices remotely.

Subnet Mask

An address code mask that determines the size of the network. An IP subnet are determined by performing a BIT-wise AND operation between the IP address and the subnet mask. By changing the subnet mask, you can change the scope and size of a network.

TFTP

Trivial File transfer Protocol. A file transfer protocol, with the functionality of a very basic form of FTP. It is used to transfer small amounts of data between hosts on a network, such as Switch firmware.